

UNIVERSITÀ DEGLI STUDI DI MILANO
FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
CORSO DI LAUREA IN MATEMATICA



Heegner points on $X_0(N)$

Thesis advisor: Prof. Jan Nekovář

Master thesis by:
Francesca Gala

Academic Year 2010/2011

Contents

Introduction	1
0 Preliminaries	4
0.1 Elliptic curves, first definitions.	4
0.2 Reduction of elliptic curves over local fields.	6
0.3 Class field theory	10
0.4 Complex Multiplication	14
1 Heegner points on $X_0(N)$	16
1.1 The modular curve $X_0(N)$	16
1.2 A moduli interpretation	20
1.3 Operators on modular curves and the Eichler-Shimura relation	21
1.4 The modular parametrisation	25
1.5 Definition of a Heegner point on $X_0(N)$	29
1.6 Heegner points on elliptic curves	33
2 Kolyvagin's Theorem	34
2.1 Galois action on torsion points	35
2.2 Construction of an 'Euler system'	37
2.3 Construction of cohomology classes.	38
2.4 Properties of the cohomology classes $c(n)$	41
2.5 Local triviality of the cohomology classes.	43
2.6 Tate local duality.	46
2.7 Computation of the Selmer group.	50
Bibliography	60

Introduction

The goal of this memoire is to explain the proof of a theorem of Kolyvagin on the group of rational points on an elliptic curve, following the exposition by Gross in his article [Gro].

An important question in the theory of elliptic curves is to determine the structure of the group of rational points of a given elliptic curve. Mordell-Weil's theorem, theorem (0.2), asserts that an elliptic curve E over a field K satisfies:

$$E(K) \simeq \mathbb{Z}^r + E(K)_{\text{tors}},$$

where $E(K)_{\text{tors}}$ is the group of torsion points on E , which can be effectively determined for a given elliptic curve.

Unfortunately it seems hard in general to have an efficient way of determining the rank.

The theorem of Kolyvagin, proposition (2.1) in this *mémoire*, asserts that for 'modular' elliptic curves over \mathbb{Q} if we can prove that a certain Heegner point $y_K \in E(K)$, definition (1.11), has infinite order in $E(K)$ then we can deduce that the rank of the curve is one.

This theorem is important for a number of different aspects.

First of all, recently Breuil, Conrad, Diamond, and Taylor proved that every elliptic curve over \mathbb{Q} is modular, that is it admits a modular parametrisation:

$$\phi : X_0(N) \longrightarrow E.$$

So Kolyvagin's theorem can be applied to every elliptic curve over \mathbb{Q} .

Moreover, in [GZ86], Gross-Zagier show that Heegner points satisfy a formula that links their height to the value in 1 of the first derivative of the L -function of the elliptic curve. As a consequence the point $y_K \in E(K)$ has infinite order if and only if $L'(E/K, 1) \neq 0$.

So Kolyvagin's theorem can be combined with Gross-Zagier's formula to give a proof of a special case of the Birch and Swinnerton-Dyer conjecture, namely the fact that if you consider an elliptic curve E over \mathbb{Q} and show that $\text{ord}_{s=1} L(E, s) \leq 1$, then you can deduce

$$\text{rank}(E(\mathbb{Q})) = \text{ord}_{s=1} L(E, s),$$

as predicted by the conjecture.

Another aspect that has to be remarked is that the technique that Kolyvagin uses in proving the theorem is very powerful and has later been generalised to a number of different situations. His method lies in the construction of an 'Euler system' of Heegner points, in the language of Kolyvagin, that is

used to bound the order of the Selmer group $\text{Sel}(E/K)$, definition (0.3), from which we can deduce information on the group of rational points.

Chapter 0 is concerned with giving some preliminaries on elliptic curves, class field theory and complex multiplication.

Chapter 1 explains a construction of the modular curve $X_0(N)$, gives some generalities on modular functions and modular forms and finally gives the definition of a Heegner point on a modular curve. These points correspond, in the moduli interpretation of $X_0(N)$, section (1.2), to couples of elliptic curves with the same ring of complex multiplication.

Chapter 2 is dedicated to the proof of a special case of Kolyvagin's theorem, proposition (2.2).

The proof, which is the prototype of a general Euler system argument, goes as follows.

First of all we show that the system of Heegner points as defined in chapter 1 satisfies the properties of being an Euler system, proposition (2.7). Then using these properties we are able to construct a system of cohomology classes, which Kolyvagin calls the 'derivative classes', that are proved to be locally trivial except maybe at some particular prime which is linked to the Heegner points, propositions (2.14) and (2.16).

The last part of the chapter is then concerned with finishing the proof by bounding the order of the p -Selmer group, with the prime p as in (2.3). First by using Galois cohomology and some results from Tate's local duality we are able to obtain information on the local components of the Selmer group from the cohomology classes. Then Chebotarev density theorem, is used to convert information on the local components of the Selmer group to an upper bound on its order.

Some comments on notation.

We will write E_p for the full group of torsion points on the algebraic closure of the field of definition of E , i.e. if E is an elliptic curve defined over a number field K then $E_p := E(\bar{K})_p$ the p -torsion of $E(\bar{K})$. More generally $(\cdot)_p$ indicates the p -torsion of group in brackets, for example we will meet $E(L)_p$ where L is a number field or a p -adic field. When using cohomology we will always intend group cohomology as defined for example in [CF67] Chap. IV and we will denote $H^n(K, E) = H^n(\text{Gal}(\bar{K}/K), E(\bar{K}))$ and $H^n(L/K, E) = H^n(\text{Gal}(L/K), E(L))$.

Chapter 0

Preliminaries

In this chapter we are going to review some basic definitions from the theory of elliptic curves, some results from class field theory and complex multiplication.

0.1 Elliptic curves, first definitions.

Definition 0.1. An *elliptic curve* over a field K is a non singular projective curve over K of genus 1 equipped with a K -rational point, $O \in K$.

By the Riemann-Roch theorem, an elliptic curve can be described explicitly as the projective non singular plane curve described by a cubic *Weierstrass equation* of the form:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \quad (0.1)$$

Remark. For any extension L of the field K , the L -rational points $E(L)$ are naturally equipped with an abelian group structure with $O \in E(K)$ as the zero element.

A major problem in the theory of elliptic curves is to actually describe the group of rational points.

We have the following result:

Theorem 0.2 (Mordell-Weil theorem). Let E be an elliptic curve over a number field K . The group of rational points $E(K)$ is finitely generated, i.e

$$E(K) \simeq E(K)_{tors} \times \mathbb{Z}^r$$

where $E(K)_{tors}$ is a finite group and $r = r(E/K)$ is called the *rank* of E .

Unfortunately the proof of this theorem doesn't provide us with a procedure to effectively compute the generators of $E(K)$.

The proof of the theorem has two steps. First of all one has to prove the

'Weak Mordell-Weil theorem' which asserts that $E(K)/pE(K)$ is finite for some prime p . Then one uses the theory of heights in the projective space to deduce that a point of $E(K)$ is not 'infinitely divisible' and so one can exhibit a set of generators of $E(K)$ knowing $E(K)/pE(K)$.

The problem of effectivity lies in the proof of the 'Weak Mordell-Weil' theorem. In fact finiteness is deduced by injecting the group $E(K)/pE(K)$ into another group, called the p -Selmer group, which one can compute and prove that it is finite, nevertheless there is not enough information on the 'difference' between these two groups. We are not able to describe in general the quotient of the p -Selmer group by $E(K)/pE(K)$, which is the p -torsion of the so-called Tate-Shafarevich group.

Let us see in detail how these groups are constructed.
Consider the exact sequence:

$$0 \rightarrow E_p \rightarrow E \xrightarrow{p} E \rightarrow 0, \quad (0.2)$$

where $(\cdot)_p$ is the p -torsion.

Taking Galois cohomology by the group $\text{Gal}(\overline{K}/K)$ one obtains:

$$0 \rightarrow E(K)_p \rightarrow E(K) \xrightarrow{p} E(K) \rightarrow H^1(K, E_p) \rightarrow H^1(K, E) \xrightarrow{p} H^1(K, E) \rightarrow \dots$$

From which one deduces the following short exact sequence:

$$0 \rightarrow E(K)/pE(K) \rightarrow H^1(K, E_p) \rightarrow H^1(K, E)_p \rightarrow 0 \quad (0.3)$$

Now consider a prime v of K and let K_v be the completion of K at v , $\text{Gal}(\overline{K}_v/K_v)$ can be seen as a decomposition group of $\text{Gal}(\overline{K}/K)$, so that $\text{Gal}(\overline{K}_v/K_v) \hookrightarrow \text{Gal}(\overline{K}/K)$.

So considering the morphism of restriction in cohomology one has the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{f} & H^1(K, E)_p \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow g \\ 0 & \longrightarrow & \prod_v E(K_v)/pE(K_v) & \longrightarrow & \prod_v H^1(K_v, E_p) & \longrightarrow & \prod_v H^1(K_v, E)_p \longrightarrow 0 \end{array} \quad (0.4)$$

Notation. When we write $H^1(K, E)$, by E we mean $E(\overline{K})$ and similarly for $H^1(K_v, E)$.

Definition 0.3. The p -Selmer group of E/K is the kernel of $g \circ f$, i.e.

$$\text{Sel}_p(E/K) = \ker(H^1(K, E_p)) \rightarrow \prod_v H^1(K_v, E)_p$$

Definition 0.4. The p -torsion of the *Tate-Shafarevich group* is the kernel of g . We can define the *Tate-Shafarevich group* to be:

$$\text{III}(E/K) = \ker(\text{H}^1(K, E) \rightarrow \prod_v \text{H}^1(K_v, E))$$

From these definitions we can deduce the following *descent sequence*:

$$0 \rightarrow E(K)/pE(K) \xrightarrow{\delta} \text{Sel}_p(E/K) \rightarrow \text{III}(E/K)_p \rightarrow 0, \quad (0.5)$$

where the map δ sends a class $[P]$ to the cocycle:

$$\begin{aligned} \delta(P) : \text{Gal}(\overline{K}/K) &\longrightarrow E_p \\ \sigma &\longmapsto \sigma\left(\frac{1}{p}P\right) - \frac{1}{p}P. \end{aligned}$$

0.2 Reduction of elliptic curves over local fields.

Throughout this section let R denote a complete discrete valuation ring, $L = \text{Frac}R$ its fraction field, $\pi \in R$ a uniformizing element which generates the maximal ideal $\mathfrak{m} = (\pi)$ and $k = R/\mathfrak{m}R$ the residue field of characteristic l .

We assume that L is complete with respect to the valuation.

Given an elliptic curve E we wish to find a model \mathcal{E} of E over R .

Definition 0.5. Let E be an elliptic curve over L .

A *minimal Weierstrass model* of E over R is a generalized Weierstrass equation

$$\mathcal{W} : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

of an elliptic curve \mathcal{W} isomorphic to E such that:

1. all the $a_i \in R$ and
2. $\text{ord}_\pi(\Delta(\mathcal{W}))^1 \geq 0$ is minimal (among all the \mathcal{W} as above which satisfy 1.)

Remark. We have in particular from the definition that:

$$\mathcal{W}(R) \simeq E(L).$$

Now we would like to analyze the reduction of the model \mathcal{W} of E over the residue field k .

¹Considering the coefficients of the affine form of the equation for \mathcal{W}

$$f(x, y) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

as variables, the intersection of the ideal $(f, \partial f/\partial x, \partial f/\partial y)$ in $\mathbb{Z}[x, y, a_1, \dots, a_6]$ with $\mathbb{Z}[a_1, \dots, a_6]$ is a principal ideal, generated by a polynomial $\Delta(a_1, \dots, a_6) \in \mathbb{Z}[a_1, \dots, a_6]$. $\Delta = \Delta(\mathcal{W})$ is precisely the discriminant of \mathcal{W} , unique up to sign.

Definition 0.6. Let E be an elliptic curve over L ; fix a minimal Weierstrass model \mathcal{W} over R . The *reduction* of E over k is $\tilde{E} := \mathcal{W} \otimes_R k$, i.e.

$$\tilde{E} : y^2z + \bar{a}_1xyz + \bar{a}_3yz^2 = x^3 + \bar{a}_2x^2z + \bar{a}_4xz^2 + \bar{a}_6z^3,$$

where $\bar{a}_i \in k$ are the reduction of the a_i s modulo \mathfrak{m} .

Remark. 1. \tilde{E} is a cubic projective curve over k . Its discriminant is equal to $\Delta(\tilde{E}) = \Delta(\mathcal{W}) \bmod \pi$.

2. The isomorphism class of \tilde{E} does not depend on \mathcal{W} , only on E .

Definition 0.7. We say that E has *good reduction* over R if $\text{ord}_\pi(\Delta(\mathcal{W})) = 0$, i.e. if $\Delta(\tilde{E}) \neq 0$ which means that \tilde{E} is an elliptic curve over k .

We say that E has *bad reduction* over k if $\pi | (\Delta(\mathcal{W}))$, which means that \tilde{E} is not smooth over k .

Consider the reduction map on the elliptic curve:

$$\text{red} : E(L) \simeq \mathcal{W}(R) \longrightarrow \tilde{E}(k),$$

which is obtained by sending a point $(a : b : c) \in \mathcal{W}(R)$ to the point $(\bar{a} : \bar{b} : \bar{c}) \in \tilde{E}(k)$, where \bar{a} is the reduction of $a \in R \bmod \pi$.

Let us assume that if E has bad reduction, then its unique non-smooth point S is defined over k . This assumption is automatically satisfied if $\text{char } k \neq 2, 3$ or if k is perfect.

Let:

$$\tilde{E}^{\text{sm}} = \begin{cases} \tilde{E} & \text{if } E \text{ has good reduction.} \\ \tilde{E} \setminus \{S\} & \text{if } E \text{ has bad reduction.} \end{cases}$$

It can be proved that there there exists a group law on $\tilde{E}_{\text{sm}}(k)$, which makes it a group variety.

Proposition 0.8. Let $E_0(L) = \text{red}^{-1}(\tilde{E}^{\text{sm}}(k))$, then there exists an exact sequence of abelian groups:

$$0 \rightarrow E_1(L) \longrightarrow E_0(L) \xrightarrow{\text{red}} \tilde{E}^{\text{sm}}(k) \rightarrow 0, \quad (0.6)$$

where $E_1(L) = \ker(\text{red})$.

We can say something more about $E_1(L)$:

Proposition 0.9. Let \widehat{E} over R be the formal² group associated to E then there exists an isomorphism of groups:

$$E_1(L) \longrightarrow \widehat{E}(\pi R).$$

Moreover $E_1(L) \simeq \widehat{E}(\pi R)$ is a pro- l -group. ($l = \text{char } k$)

²See [Sil09] Chap. IV and Prop. 2.2 Chap. VII

Now consider the case of an elliptic curve E , which has good reduction over L .

Then sequence (0.6) becomes:

$$0 \rightarrow E_1(L) \rightarrow E(L) \rightarrow \tilde{E}(k) \rightarrow 0 \quad (0.7)$$

Now suppose that m is an integer prime to l . Then, by the fact that E_1 is pro- l we have that multiplication by m induces an isomorphism on $E_1(L)$. So we have the following commutative diagram:

$$\begin{array}{ccccccccc}
& & 0 & \longrightarrow & E(L)_m & \longrightarrow & \tilde{E}(k)_m & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_1(L) & \longrightarrow & E(L) & \longrightarrow & \tilde{E}(k) & \longrightarrow & 0 \\
& & \sim \downarrow m & & \downarrow m & & \downarrow m & & \\
0 & \longrightarrow & E_1(L) & \longrightarrow & E(L) & \longrightarrow & \tilde{E}(L) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
& & 0 & \longrightarrow & E(L)/mE(L) & \longrightarrow & \tilde{E}(k)/m\tilde{E}(k) & \longrightarrow & 0
\end{array}$$

From which we can deduce:

$$E(L)/mE(L) \xrightarrow{\sim} \tilde{E}(k)/m\tilde{E}(k) \quad (0.8)$$

and

$$E(L)_m \xrightarrow{\sim} \tilde{E}(k)_m. \quad (0.9)$$

Moreover if L is replaced with an extension M large enough to contain all of $E(\bar{L})_m$, then:

$$E_m := E(\bar{L})_m \simeq \tilde{E}(k^{\text{sep}})_m.$$

We want to give an idea of the reason why minimal Weierstrass models \mathcal{W} do not seem to be sufficient. The problem is when E has bad reduction. In that case we have seen that \tilde{E} is not smooth over k , so \mathcal{W} is not 'smooth', in scheme-theoretical language, and the group law over \mathcal{W} is not a morphism, which implies that \mathcal{W} is not a group scheme. On the other hand if we consider $\mathcal{W}^0 (\simeq E_0(L))$, the largest subscheme of \mathcal{W} which is 'smooth' over R , it can be proved that there exists a morphism $\mathcal{W}^0 \times \mathcal{W}^0 \rightarrow \mathcal{W}^0$ which makes it a group scheme, but we have lost the point extension property, i.e. $\mathcal{W}^0(R) \neq E(L)$.

What we would like to find is a 'smooth' scheme \mathcal{E} over $\text{Spec}R$ such that:

1. $\mathcal{E}(R) \simeq E(K)$ and
2. the group law on E extends to a morphism $\mathcal{E} \times_R \mathcal{E} \rightarrow \mathcal{E}$.

We give the definition of a Néron model in a greater generality than the hypothesis of the section, i.e. when R is a Dedekind domain.

Definition 0.10. Let L be the fraction field of a Dedekind domain R . Let E be an elliptic curve over L . A *Néron model* \mathcal{E} of E is a smooth separated scheme over R such that:

1. Its generic fibre is E , i.e. there is a cartesian diagram

$$\begin{array}{ccc} E \simeq \mathcal{E} \times_R \text{Spec}(L) & \longrightarrow & \mathcal{E} \\ \downarrow & & \downarrow \\ \text{Spec}(L) & \longrightarrow & \text{Spec}(R) \end{array}$$

2. The scheme \mathcal{E} has the following universal property:

For any smooth scheme $X \rightarrow R$ and any morphism $\psi_K : X \times_R \text{Spec}(L) \rightarrow E$ there is a unique morphism $\psi : X \rightarrow \mathcal{E}$ such that:

$$\psi \times_R \text{Spec}(L) = \psi_K,$$

i.e. the following diagram is commutative:

$$\begin{array}{ccc} X \times_R \text{Spec}(L) & \longrightarrow & X \\ \psi_K \downarrow & & \downarrow \psi \\ E \simeq \mathcal{E} \times_R \text{Spec}(L) & \longrightarrow & \mathcal{E} \end{array}$$

Theorem 0.11. Let E be an elliptic curve as in definition (0.10), then a Néron model \mathcal{E} over R exists.

Proof. A proof may be found in [Art86] of the general case of abelian varieties or in [Sil94] Chap. IV for the special case of elliptic curves. \square

- Remark.**
1. 'The' Néron model is unique by the universal property.
 2. There is a group scheme structure on \mathcal{E} over R extending the group variety structure on E .
 3. As a particular case of the universal property, i.e. when $X = \text{Spec}(K)$, we have:

$$\mathcal{E}(R) \simeq E(K)$$

Example 0.12. If E is an elliptic curve over a number field K such that E has good reduction over a prime v , i.e. E has good reduction over the ring \mathcal{O}_{K_v} , then a minimal Weierstrass model \mathcal{W} as defined in (0.5) is a Néron Model \mathcal{E} for E over \mathcal{O}_{K_v} .

When E has bad reduction, as we have already remarked, the Néron model is in general quite different from the smooth part of a minimal Weierstrass model, which is, in fact, the connected component of the identity of the Néron model.

Let us now define the conductor of an elliptic curve in the special case of an elliptic curve defined over \mathbb{Q} :

Definition 0.13. Let E be an elliptic curve over \mathbb{Q} . Define the quantity³ f_p as follows:

$$f_p = \begin{cases} 0, & \text{if } E \text{ has good reduction at } p, \\ 1, & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 + \delta_p, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

where δ_p is a 'measure' of the wild ramification in the action of the inertia group on the Tate-module $T_p(E)$.

The *conductor* of an elliptic curve E over \mathbb{Q} is:

$$N_{E/\mathbb{Q}} = \prod_p p^{f_p}.$$

Now we end this section with a definition.

Definition 0.14. Let E be an elliptic curve over \mathbb{Q} and \tilde{E} the reduction of the Néron model of E over \mathbb{Z}_p .

Write n_p for the order of the group of \mathbb{F}_p -rational non-singular points of $\tilde{E}(\mathbb{F}_p)$. Then set:

$$a_p = \begin{cases} p + 1 - n_p, & \text{if } p \text{ does not divide } N, \\ p - n_p & \text{otherwise.} \end{cases}$$

The L -series of E over \mathbb{Q} is the function of the complex variable s defined by:

$$L(E, s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N} (1 - a_p p^{-s})^{-1}.$$

0.3 Class field theory

In this section we refer to [Cox97] for an informal approach to the theory and to [CF67] Chapter VII for more accurate statements and for proofs.

Let K be a number field. We shall indicate with the word 'prime' in K an equivalence class of non-trivial valuations of K . There is a distinction between primes which are 'finite', represented by prime ideals in \mathcal{O}_K , and primes which are 'infinite', that can be real, represented by an embedding $K \hookrightarrow \mathbb{R}$, or complex, represented by a couple of complex conjugate embeddings of K into \mathbb{C} .

Recall that a modulus \mathfrak{m} in K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

³For a definition of multiplicative and additive reduction see [Sil09] Chap. VII Prop. 5.1. Let us simply note that if E has *multiplicative*, or *additive*, *reduction* at p then the singular point of the reduction of E modulo p has a node or a cusp respectively.

such that $n_{\mathfrak{p}} \geq 0$ for all \mathfrak{p} and $n_{\mathfrak{p}} = 0$ for all but finitely many, if \mathfrak{p} is real $n_{\mathfrak{p}} = 0$ or 1 and if \mathfrak{p} is complex then $n_{\mathfrak{p}} = 0$.

We can factorise a modulus $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$, where finite primes divide \mathfrak{m}_0 and infinite ones \mathfrak{m}_∞ .

Definition 0.15. Let

$$P_{K,1}(\mathfrak{m}) = \{a \in K^\times \mid v_{\mathfrak{p}}(a-1) \geq n_{\mathfrak{p}} \ \forall \mathfrak{p} \mid \mathfrak{m}_0 \text{ and } \sigma(a) > 0 \ \forall \sigma = \mathfrak{p} \mid \mathfrak{m}_\infty\}$$

and $I_K(\mathfrak{m})$ be the set of fractional ideals of K generated by the prime ideals which do not divide \mathfrak{m} .

Every $a \in P_{K,1}(\mathfrak{m})$ defines a principal ideal in $I_K(\mathfrak{m})$, so we can define the *ray class group* modulo \mathfrak{m} :

$$C_{\mathfrak{m}} = \frac{I_K(\mathfrak{m})}{P_{K,1}(\mathfrak{m})}.$$

Let L/K be a finite Galois extension.

For any prime ideal \mathfrak{p} of K that is unramified in L and for \mathfrak{q} which lies above \mathfrak{p} in L , there exists an element $\sigma = (\mathfrak{q}, L/K)$ of $\text{Gal}(L/K)$ uniquely determined by the condition that $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{q}}$ for any $\alpha \in \mathcal{O}_L$. Moreover it can be proven that for all the prime ideals \mathfrak{q} lying above \mathfrak{p} , the symbols $(\mathfrak{q}, L/K)$ are conjugate to one another.

In particular if L/K is an abelian extension then the set $\{(\mathfrak{q}, L/K) \text{ s. t. } \mathfrak{q} \mid \mathfrak{p}\}$ is composed of only one element which we call the *Frobenius element*:

$$\text{Frob}(\mathfrak{p}) := (\mathfrak{p}, L/K) = (\mathfrak{q}, L/K)$$

for any \mathfrak{q} lying above \mathfrak{p} .

Definition 0.16. Let L/K be an abelian extension.

For any modulus \mathfrak{m} which is divisible by all the primes that ramify in L we have a homomorphism

$$\begin{aligned} \psi_{L/K} : \quad I_K(\mathfrak{m}) &\longrightarrow \text{Gal}(L/K) \\ \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t} &\longmapsto \prod_i (\mathfrak{p}_i, L/K)^{n_i} \end{aligned} \quad (0.10)$$

called the *Artin map* (or reciprocity map).

Remark. A prime ideal splits completely in K if and only if it is in the kernel of the Artin map.

Now recall the definition of the norm map $N_{L/K} : I_L \rightarrow I_K$, which sends a prime ideal \mathfrak{q} of L to $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})}$ where $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ and $f(\mathfrak{q}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = [\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}]$ is the residue degree.

By direct computation, it can be deduced that the image of I_L by the norm map is in the kernel of the Artin map, i.e.

$$N_{L/K}(I_L) \subset \ker \psi_{L/K}.$$

Now we can state the first main theorem of class field theory.

Theorem 0.17. [Artin reciprocity law] Let L/K be a finite abelian extension. There exists a modulus \mathfrak{m} of K which satisfies the following properties:

- a. It is divisible by all the primes of K that ramify in L ,
- b. $P_{K,1}(\mathfrak{m}) \subset \ker \psi_{L/K}$

and is such that the following holds for the Artin map

$$\psi_{L/K} : I_K(\mathfrak{m}) \longrightarrow \text{Gal}(L/K)$$

- 1. It is surjective,
- 2. $\ker \psi_{L/K} = P_{K,1}(\mathfrak{m}) \cdot N_{L/K}(I_L(\mathfrak{m}'))$, where \mathfrak{m}' is divisible by all primes of L which lie above primes of \mathfrak{m} .

Remark. The minimal modulus \mathfrak{m} among the ones which satisfy properties a. and b. of the theorem is called the *conductor* of the extension.

Now we need a result which tells us something about the existence of such abelian extensions as in the previous theorem.

Definition 0.18. A subgroup H of $I_K(\mathfrak{m})$ is called a *congruence subgroup modulo \mathfrak{m}* if

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Theorem 0.19 (Existence theorem). Let \mathfrak{m} be a modulus of K and let H be a congruence subgroup for \mathfrak{m} .

Then there exists a unique abelian extension L/K , all of whose ramified primes divide \mathfrak{m} , such that

$$H = P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}')),$$

\mathfrak{m}' as in 2. of theorem 0.17, i.e. the Artin map induces:

$$\psi_{L/K} : \frac{I_K(\mathfrak{m})}{H} \xrightarrow{\sim} \text{Gal}(L/K).$$

Example 0.20 (Hilbert class field). Consider the trivial modulus $\mathfrak{m} = 1$ and the subgroup P_K of principal ideals, which is trivially a congruence subgroup, then the theorem predicts us the existence of an abelian extension K_1 of K unramified everywhere. We call this extension the *Hilbert class field* of K .

Example 0.21 (Ring class field of conductor n). Consider an order $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ of conductor n in an imaginary quadratic field K , in which we suppose for simplicity that $\mathcal{O}_K^\times = \{\pm 1\}$. Let $\text{Pic}(\mathcal{O}_n)$ be the group of projective modules of rank 1 over \mathcal{O}_n , this is the same as:

$$\text{Pic}(\mathcal{O}_n) \simeq \text{Cl}(\mathcal{O}_n) \simeq \frac{I_K(n)}{P_{K,\mathbb{Z}}(n)},$$

Theorem 0.22 (Chebotarev density theorem). Let L/K be a finite Galois extension. Let $\langle \sigma \rangle$ be the conjugacy class of an element $\sigma \in \text{Gal}(L/K)$. Then the set of unramified prime ideals of K such that $(\mathfrak{p}, L/K) = \langle \sigma \rangle$ has Dirichlet density⁴:

$$\frac{|\langle \sigma \rangle|}{|\text{Gal}(L/K)|} = \frac{|\langle \sigma \rangle|}{[L : K]}.$$

In particular, if L/K is abelian, then the set of unramified primes such that $\text{Frob}(\mathfrak{p}) = \sigma$ has density $1/[L : K]$, and hence is infinite.

0.4 Complex Multiplication

An important problem in algebraic number theory is to give an explicit description of all abelian extensions of a given number field K . For instance, the theorem of Kronecker-Weber gives a characterisation of the maximal abelian extension of \mathbb{Q} .

The theory of complex multiplication does essentially the same thing for an imaginary quadratic number field K .

For the proofs of this section see [Cox97] or [CF67] Chap XIII.

Throughout this section we consider elliptic curves defined over \mathbb{C} .

Definition 0.23. $E \simeq \mathbb{C}/\Lambda$ is said to have *complex multiplication* if there exists an element $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ such that $\alpha\Lambda \subset \Lambda$, or equivalently if $\text{End}(E) \otimes \mathbb{Q} = K$ is an imaginary quadratic field.

Remark. In the case when E has complex multiplication, $\text{End}(E)$ will be an order \mathcal{O} in K , i.e. $\mathcal{O} = \mathbb{Z} + n\mathcal{O}_K$, with $n \in \mathbb{Z}$ the *conductor* of the order.

Proposition 0.24. Elliptic curves with complex multiplication by a given endomorphism ring \mathcal{O} correspond, up to isomorphism, to elements of $\text{Pic}(\mathcal{O})$. The correspondence is given by:

$$\mathbb{C}/\mathfrak{a} \mapsto \mathfrak{a}.$$

To each E we can associate an invariant $j(E) \in \mathbb{C}$, called the *j -invariant*, which classifies elliptic curves up to isomorphism.

Let $E \simeq \mathbb{C}/\Lambda$, with $\Lambda = [\omega_1, \omega_2]$, then $j(E) = j(\Lambda)$ can be defined as follows:

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} \quad (0.13)$$

⁴Recall the definition of Dirichlet density $\delta(S)$ of a subset S of the set of finite primes M_K of a number field K :

$$\delta(S) := \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

provided that the limit exists.

where

$$g_2(\Lambda) = 60 \sum_{(m,n) \neq (0,0)} \frac{1}{(m\omega_1 + n\omega_2)^4} \text{ and } g_3(\Lambda) = 140 \sum_{(m,n) \neq (0,0)} \frac{1}{(m\omega_1 + n\omega_2)^6}.$$

We call the denominator of the j -invariant the *discriminant* of Λ :

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \quad (0.14)$$

Remark. The j -invariant that we have just defined can be associate to every invertible ideal $\mathfrak{a} \in \text{Pic}(\mathcal{O})$, by considering $j(\mathfrak{a}) = j(\mathbb{C}/\mathfrak{a})$ and it can be proved that j depends only on the ideal class of \mathfrak{a} .

Theorem 0.25. Let E be an elliptic curve complex multiplication by an order \mathcal{O}_n of conductor n in an imaginary quadratic field K . Then the following holds:

1. $j(E)$ is an algebraic number,
2. $K(j(E))$ is the ring class field of K of conductor n ,
3. If $\mathcal{O}_n = \mathcal{O}_K$, i.e. if $n = 1$, then $K(j(E))$ is the Hilbert class field of K , as defined in example (0.20).

We are now interested in being a little more explicit, we would like to better understand the isomorphism:

$$\begin{array}{ccc} \text{Pic}(\mathcal{O}_n) & \xrightarrow{\sim} & \text{Gal}(K(j(\Lambda))/K) \\ \mathfrak{p} & \longmapsto & \text{Frob}(\mathfrak{p}) \end{array}$$

Theorem 0.26. Let \mathcal{O} be an order of conductor n in K . Consider the elliptic curve E/\mathfrak{a} with $\mathfrak{a} \in \text{Pic}(\mathcal{O}_n)$. Let \mathfrak{p} be a prime ideal of \mathcal{O}_K , with norm prime to n , and let

$$\mathfrak{p}_n = \mathfrak{p} \cap \mathcal{O}_n.$$

Then the Frobenius element $\text{Frob}(\mathfrak{p})$ acts on $j(\mathfrak{a})$ by:

$$\text{Frob}(\mathfrak{p})(j(\mathfrak{a})) = j(\mathfrak{a} \cdot \mathfrak{p}_n^{-1}).$$

Chapter 1

Heegner points on $X_0(N)$

In this chapter we are going to explain a construction of the modular curve $X_0(N)$ and show the existence of a system of points on it, the so-called Heegner points, which are defined over certain ring class fields.

1.1 The modular curve $X_0(N)$

Consider the upper half plane $\mathcal{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$. The group of matrices $\text{GL}_2^+(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc > 0 \right\}$ acts on \mathcal{H} by:

$$\gamma \cdot \tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

For our purposes we want to consider only the action of a certain subgroup of $\text{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$ namely the *Hecke congruence subgroup* of level N , for $N \in \mathbb{N}$:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

Remark. $\Gamma_0(1) = \text{SL}_2(\mathbb{Z})$.

Proposition 1.1. The quotient $\mathcal{H}/\Gamma_0(N)$ can be given a natural structure of a Riemann surface.

Definition 1.2. Let $Y_0(N)$ be the Riemann surface such that:

$$Y_0(N) \simeq \mathcal{H}/\Gamma_0(N)$$

Moreover, we can compactify and obtain:

Definition 1.3. Let $X_0(N)$ be the Riemann surface obtained as the compactification of $Y_0(N)$, namely

$$X(\mathbb{C}) \simeq \mathcal{H}^*/\Gamma_0(N),$$

where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ and $\Gamma_0(N)$ acts on $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{m}{n} = \frac{am + bn}{cm + dn}$$

with the convention that

$$\frac{a\infty + b}{c\infty + d} = \frac{a}{c}.$$

The points in the finite set $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N) = X_0(N) \setminus Y_0(N)$ are called the *cusps* of X .

Now our interest lies in better understanding these curves and to do so we investigate on the functions and differentials that can be defined on them.

In this direction we give two basic definitions.

Definition 1.4. A meromorphic function $f : \mathcal{H} \rightarrow \mathbb{C}$ is a *modular function* for $\Gamma_0(N)$ if:

- i. $f(\gamma\tau) = f(\tau)$ for any $\gamma \in \Gamma_0(N)$,
- ii. $f(\gamma\tau)$ is meromorphic at the cusps for all $\gamma \in \text{SL}_2(\mathbb{Z})$, i.e. the q -expansion of $f(\gamma\tau)$ at ∞ involves only a finite number of non negative powers of q .

Remark. a. Thanks to condition i, condition ii has to be checked only for a finite number of elements of $\text{SL}_2(\mathbb{Z})$, the representatives of the cosets of $\Gamma_0(N)$ in $\text{SL}_2(\mathbb{Z})$.

b. Condition ii tells us that we can see f as a meromorphic function defined on $X_0(N)$.

Example 1.5. We can consider the j -invariant defined in (0.13) as a function $j : \mathcal{H} \rightarrow \mathbb{C}$ by sending $\tau \in \mathcal{H}$ to $j(\tau) = j([1, \tau])$.

The function j is a modular function for $\text{SL}_2(\mathbb{Z})$.

Moreover we can define another function $j_N : \mathcal{H} \rightarrow \mathbb{C}$, by sending $\tau \in \mathcal{H}$ to

$$j_N(\tau) := j(N\tau).$$

j_N is a modular function for $\Gamma_0(N)$.

Definition 1.6. Let k be an integer. A meromorphic function $f : \mathcal{H} \rightarrow \mathbb{C}$ is a *modular form of weight k* for $\Gamma_0(N)$ if:

- i. f is holomorphic on \mathcal{H} ,
- ii. $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$,

iii. $f(\gamma\tau)$ is holomorphic at the cusps for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, i.e. the q -expansion of

$$f|_k\gamma(\tau) = (c\tau + d)^{-k}f(\gamma\tau)$$

at ∞ involves only non negative powers of q .

Definition 1.7. A *cuspidal form of weight k* is a modular form of weight k for which the q -expansion of $(f|_k\gamma)(\tau) = \sum a_n q^n$ at the cusps is such that $a_0 = 0$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Notation. We will indicate by $S_k(\Gamma_0(N))$ the space of weight k cusp forms for $\Gamma_0(N)$.

Example 1.8. The discriminant $\Delta(\Lambda)$ as defined in (0.14) can be seen as a modular form by sending $\tau \in \mathbb{C}$ to $\Delta(\tau) = \Delta([1, \tau])$. It can be proved that $\Delta(\tau)$ is a cuspidal form of weight 12.

The next theorem characterises completely modular functions for $\Gamma_0(N)$.

Theorem 1.9. Let $N \in \mathbb{N}$. Every modular function for $\Gamma_0(N)$ is a rational function of j and j_N .

Proof. (idea of)

Step 1. Every modular function g for $\mathrm{SL}_2(\mathbb{Z})$ is a rational function of j .

First of all one has to prove that every holomorphic modular function f for $\mathrm{SL}_2(\mathbb{Z})$ is a polynomial in j . This is done by first showing that if f is holomorphic at ∞ , then it is constant; indeed in this case $f(\mathcal{H} \cup \{\infty\})$ is compact so that we can conclude by the maximum modulus principle. Then since the q -expansion of $j(\tau)$ begins with $1/q$ we can always find a polynomial $A(j(\tau))$ such that $f(\tau) - A(j(\tau))$ is holomorphic at ∞ . Step 1 follows by showing the existence of a polynomial $B(j)$ such that $B(j(\tau))g(\tau)$ is a holomorphic modular function.

Step 2. Introducing the modular equation.

Let $n = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ and explicitly compute a set of representatives for the right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, call them: $\{\Gamma_0(N)\gamma_i\}$ for $i = 1, \dots, n$.

Then fix $\tau \in \mathcal{H}$ and consider the polynomial in the variable X :

$$\Phi_N(X, \tau) = \prod_{i=1}^n (X - j(N\gamma_i\tau)),$$

it can be proved that $\Phi_N(X, \tau)$ is a polynomial in X and $j(\tau)$ since it is easy to prove that the coefficients of X are holomorphic modular functions for $\mathrm{SL}_2(\mathbb{Z})$. So there exists a polynomial $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$ such that $\Phi_N(X, j(\tau)) = \prod_{i=1}^n (X - j(N\gamma_i\tau))$.

The equation

$$\Phi_N(X, Y) = 0 \tag{1.1}$$

is called the *Modular equation*.

Now if one introduces:

$$C_N = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid ad = N, a > 0, 0 \leq b < d, (a, b, d) = 1 \right\}$$

then it is easy to show that $j(N\gamma_i\tau)$ can be written uniquely as $j(\sigma\tau)$ with $\sigma \in C_N$.

In particular $j(N\tau) = j(\sigma\tau)$ where $\sigma = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in C_N$ so we have:

$$\Phi_N(j(\tau), j(N\tau)) = 0.$$

Step 3. Conclusion.

To finish the proof, using the modular equation one exhibits an expression for $f(\tau)$ as a rational function of j_N and j . \square

Remark. The modular equation introduced in the proof of theorem (1.9) has some very interesting properties:

1. It is irreducible over \mathbb{C} and takes coefficients in \mathbb{Z} , i.e. $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$.
2. If $x, y \in \mathbb{C}$, $\Phi_N(x, y) = 0$ if and only if there is a lattice Λ and a cyclic sublattice $\Lambda' \subset \Lambda$ of index N such that $\Phi_N(j(\Lambda'), j(\Lambda)) = 0$.

This theorem tells us that the field of meromorphic functions on $X_0(N)$ is $\mathbb{C}(j, j_N)$. We know from the theory of Riemann surfaces that $X_0(N)$ is biholomorphic to the complex points of a unique non-singular projective curve, which has $\mathbb{C}(j, j_N)$ as its field of rational functions. A remarkable property of this curve, which we shall now explain, is that it can be defined over \mathbb{Q} . Let us see how to construct this curve. Consider the curve C defined over \mathbb{Q} by the modular equation $\Phi_N(X, Y) = 0 \in \mathbb{Z}[X, Y]$ (property 1. of the above remark). This curve is singular, but we can find a non-singular projective curve X , which is isomorphic to C over \mathbb{Q} outside the locus of singularity of C . Then there exists a natural biholomorphic map:

$$\beta : X_0(N) \xrightarrow{\sim} X(\mathbb{C}) \tag{1.2}$$

which sends, outside a finite set of points, $\tau \mapsto (j(\tau), j(N\tau))$ and we can interpret X as a model for $X_0(N)$ over \mathbb{Q} .

Remark. Unfortunately the modular equation is not easy to compute nor to work with, so in the next section we are going to describe a moduli interpretation of $Y_0(N)$, which can be used to define a model for $Y_0(N)$ over \mathbb{Q} from a more 'theoretical' point of view.

1.2 A moduli interpretation

In this section we are going to explain (without proofs) how it is possible to define a model for $Y_0(N)$ over $\mathbb{Z}[1/N]$ by interpreting it as a (partial) solution to the problem of classifying *modular pairs* $(E/S, C_N)$, where S is a $\mathbb{Z}[1/N]$ -scheme, E is an elliptic curve over S and C_N is a subgroup scheme of E isomorphic to $\mathbb{Z}/N\mathbb{Z}$.

The proofs of this section may be found in [??] or for a briefer account in [??].

Let us first analyse the case of $S = \text{Spec}(\mathbb{C})$, where the situation is much simpler.

Proposition 1.10. The points of $Y_0(N)$ are in bijection the set of isomorphism classes of couples (E, C_N) of an elliptic curve E over \mathbb{C} together with a cyclic subgroup C_N of order N .

Proof. Associate to $\tau \in \mathcal{H}$ the pair:

$$\left(\frac{\mathbb{C}}{\tau\mathbb{Z} + \mathbb{Z}}, \frac{\tau\mathbb{Z} + 1/N\mathbb{Z}}{\tau\mathbb{Z} + \mathbb{Z}} \right).$$

It is easy to check that any pair (E, C_N) as in the proposition is isomorphic to $\left(\frac{\mathbb{C}}{\tau\mathbb{Z} + \mathbb{Z}}, \frac{\tau\mathbb{Z} + 1/N\mathbb{Z}}{\tau\mathbb{Z} + \mathbb{Z}} \right)$ for some $\tau \in \mathcal{H}$.

Moreover two pairs:

$$\left(\frac{\mathbb{C}}{\tau\mathbb{Z} + \mathbb{Z}}, \frac{\tau\mathbb{Z} + 1/N\mathbb{Z}}{\tau\mathbb{Z} + \mathbb{Z}} \right) \simeq \left(\frac{\mathbb{C}}{\tau'\mathbb{Z} + \mathbb{Z}}, \frac{\tau'\mathbb{Z} + 1/N\mathbb{Z}}{\tau'\mathbb{Z} + \mathbb{Z}} \right)$$

are isomorphic over \mathbb{C} if and only if $\tau' \in \Gamma_0(N)\tau$. □

Remark. An equivalent point of view is to consider the points of $Y_0(N)$ in bijection with isomorphism classes of couples (E, E') of two elliptic curves over \mathbb{C} together with a cyclic N -isogeny, i.e. an isogeny $\psi : E \rightarrow E'$ such that $\ker \psi \simeq \mathbb{Z}/N\mathbb{Z}$.

Now consider the case of a general $\mathbb{Z}[1/N]$ -scheme S . Define a functor F_N :

$$F_N : \mathbb{Z}[1/N]\text{-schemes} \longrightarrow \text{Sets},$$

where to an $S \in \mathbb{Z}[1/N]$ -schemes we associate $F_N(S)$, the set of isomorphism classes of pairs $(E/S, C_N)$, where E is an elliptic curve over S and C_N is a subgroup scheme of E isomorphic to $\mathbb{Z}/N\mathbb{Z}$.

An isomorphism between two modular pairs (E, C_N) and (F, D_N) is an isomorphism $E \xrightarrow{\sim} F$ defined over S such that C_N is mapped to D_N .

This functor is not representable, but there exists what is called a 'coarse moduli scheme' for F_N , let it be $\mathcal{Y}_0(N)$. This means that, if $F_{\mathcal{Y}_0(N)}$ is the

functor $\mathrm{Hom}_{\mathbb{Z}[1/N]}(\cdot, \mathcal{Y}_0(N))$ from $\mathbb{Z}[1/N]$ -schemes to sets, then there is a natural transformation of functors

$$j : F_N \longrightarrow F_{\mathcal{Y}_0(N)}$$

with the following universal property: If Z is any other $\mathbb{Z}[1/N]$ -scheme such that there is a natural transformation

$$i : F_N \longrightarrow F_Z := \mathrm{Hom}_{\mathbb{Z}[1/N]}(\cdot, Z),$$

then i factors uniquely through j :

$$\begin{array}{ccc} F_N & \xrightarrow{i} & F_Z \\ & \searrow j & \nearrow \text{---} \\ & F_{\mathcal{Y}_0(N)} & \end{array}$$

Note that, by Yoneda's lemma, the map $F_{\mathcal{Y}_0(N)} \rightarrow F_Z$ yields a map

$$\mathcal{Y}_0(N) \rightarrow Z.$$

We have to notice that j yields a map j_S from modular pairs $(E/S, C_N)$ to $\mathcal{Y}_0(N)(S)$ which, for general S , need not be injective nor surjective. However if $S = \mathrm{Spec}(k)$, then $\mathcal{Y}_0(N)(k)$ can be identified with the set of equivalence classes of modular pairs $(E/k, C_N)$, where two pairs are deemed equivalent if they are isomorphic over the algebraic closure of k . (As we have seen in the case of \mathbb{C} in proposition (1.10)).

Notation. By abuse of notation we will still use $Y_0(N)$ to indicate the model $\mathcal{Y}_0(N)$ defined over $\mathbb{Z}[1/N]$.

Remark. There exists also a moduli interpretation for $X_0(N)$.

The extension to the cusps is obtained by including some 'degenerate' modular pairs. (see [DI95] section 9.2). So we can find a model for $X_0(N)$ over $\mathbb{Z}[1/N]$ by considering the coarse moduli scheme, which is the solution to the problem of classifying 'generalised' modular pairs.

1.3 Operators on modular curves and the Eichler-Shimura relation

In order to construct operators on modular curves it is useful to use the moduli interpretation we have given in section (1.2) and define them on the modular pairs which the modular curves classify.

Let us see the formal argument which we shall use.

Let Y_1 and Y_2 be the coarse moduli scheme of the functors F_1 and F_2 . So we have natural transformations:

$$j_1 : F_1 \longrightarrow F_{Y_1} = \mathrm{Hom}_{\mathbb{Z}[1/N]}(\cdot, Y_1)$$

and

$$j_2 : F_2 \longrightarrow F_{Y_2} = \mathrm{Hom}_{\mathbb{Z}[1/N]}(\cdot, Y_2).$$

Suppose that we define a natural transformation

$$i : F_1 \longrightarrow F_2.$$

Composition with j_2 yields a natural transformation $j_2 \circ i : F_1 \rightarrow F_{Y_2}$, so since Y_1 is the coarse moduli scheme for F_1 we obtain a commutative diagram of natural transformations:

$$\begin{array}{ccc} F_1 & \xrightarrow{j_2 \circ i} & F_{Y_2} \\ & \searrow j_1 & \nearrow i' \\ & & F_{Y_1} \end{array}$$

i' in turn comes from a map

$$Y_1 \longrightarrow Y_2.$$

Thus any natural transformation of functors yields a canonical map of their coarse moduli schemes.

If in addition the Y_i are smooth with projective closures X_i then there is an induced map:

$$X_1 \longrightarrow X_2.$$

Let us now define some operators on modular curves.

Remark. We are going to define these operators on the open modular curve $Y_0(N)$ and assume that they can be naturally extended to the cusps, in order to have operators on $X_0(N)$.

Let the integer N have the factorisation $N = ab$, with a and b relatively prime. We will define a map

$$w_a : Y_0(N) \longrightarrow Y_0(N)$$

called the *Atkin-Lehner operator*, by defining a natural transformation from F_N to F_N .

Let K be a field containing \mathbb{Q} and let (E_K, C_N) be a modular pair. The group C_N has a unique decomposition $C_N = C_a + C_b$ as a product of a cyclic group of order a and a cyclic group of order b , since a and b are relatively

prime.

We define w_a to be the natural transformation that sends:

$$w_a : (E, C_N) \mapsto (E/C_a, E[a] + C_b/C_a),$$

where, since $C_a \cap C_b = \{1\}$ and $E[a] \simeq \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/a\mathbb{Z}$, $E[a] + C_b/C_a$ is cyclic of order N .

It can be easily seen that $w_a^2 = 1$.

Remark. In the case of $b = 1$, w_N sends

$$w_N : (E, C_N) \mapsto (E/C_N, E[N]/C_N),$$

where if $E \xrightarrow{\phi} E/C_N$ is the isogeny with $\ker \phi = C_N \simeq \mathbb{Z}/N\mathbb{Z}$, then $E/C_N \xrightarrow{\psi} E/E[N]$ is just the dual isogeny.

Let us now turn to Hecke operators. Fix a prime p not dividing N . Let us define a map:

$$Y_0(Np) \xrightarrow{(\alpha, \beta)} Y_0(N) \times Y_0(N),$$

by defining a natural transformation:

$$(E, C_N, C_p) \mapsto ((E, C_N), (E/C_p, C_N + C_p/C_p)) \quad (1.3)$$

where α is a degeneracy map which forgets the subgroup C_p . Define the *Hecke operator* T_p as the image of the map (α, β) :

$$T_p = \text{Im}(\alpha, \beta).$$

Remark. As before, we are cheating on the construction since we have not defined a model for $Y_0(Np)$ over $\mathbb{Z}_{(p)}$. Furthermore we would like to have a map:

$$X_0(Np) \xrightarrow{(\alpha, \beta)} X_0(N) \times X_0(N).$$

Unfortunately we do not have enough time or preparation to go into the details of these constructions. So we will assume to have such a well defined map on $X_0(Np)$, which acts as (1.3) on points of $Y_0(Np)$, and that can be reduced modulo p .

We can also interpret T_p as a multivalued map, or better yet as a 'correspondence',

$$X_0(N) \dashrightarrow X_0(N),$$

which sends a modular pair $(E, C_N) \in X_0(N)$ to

$$\sum_{(E, C_N, C_{p_i}) \in S} (E/C_{p_i}, C_N + C_{p_i}/C_{p_i})$$

where

$$S = \{\beta(E, C_N, C_p) \text{ where } (E, C_N, C_p) \in \alpha^{-1}(E, C_N)\}.$$

Equivalently, consider the embedding of the modular curve $X_0(N)$ into its Jacobian:

$$X_0(N) \hookrightarrow J(X_0(N)),$$

which sends the cusp (∞) to the origin of $J(X_0(N))$, so that an arbitrary point $x \in X_0(N)$ is mapped to the divisor class $(x) - (\infty)$.

T_p can be seen as a map on the Jacobian:

$$\begin{aligned} J(X_0(N)) &\longrightarrow J(X_0(N)) \\ (E, C_N) &\longmapsto \sum_{(E, C_N, C_{p_i}) \in S} (E/C_{p_i}, C_N + C_{p_i}/C_{p_i}), \end{aligned}$$

Remark. We can also extend the definition of the Hecke operators T_p when $p|N$, by sending a modular pair (E, C_N) to the sum

$$\sum_{(E, C_N, C_{p_i}) \in S} (E/C_{p_i}, C_N + C_{p_i}/C_{p_i}),$$

with the additional condition that the sum is taken over the cyclic groups C_{p_i} , which have trivial intersection with C_N .

Proposition 1.11 (The Eichler-Shimura congruence relation). The Hecke operator over \mathbb{F}_p satisfies:

$$T_p = \text{Fr}_p + \widehat{\text{Fr}}_p \text{ on } Y_0(N)_{/\mathbb{F}_p}$$

where Fr_p is the graph of Frobenius morphism in characteristic p , which sends a point $(E, C_N) \in Y_0(N)_{/\mathbb{F}_p}$ to $\text{Fr}_p(E, C_N) = (E^{(p)}, C_N^{(p)})$ and $\widehat{\text{Fr}}_p$ is the dual morphism.

Furthermore, we can obtain the same relation on $X_0(N)_{/\mathbb{F}_p}$.

Proof. Since the number of supersingular curves is finite, we can restrict our attention to the dense subset $Y_0(N)_{/\mathbb{F}_p}^{\text{ord}}$ of points on $Y_0(N)$ which are represented by ordinary elliptic curves. It will be enough to show the relation over these points to prove the proposition.

Let $(E, C_N) \in Y_0(N)_{/\mathbb{F}_p}^{\text{ord}}$ be one of these points. Call $\{C_{p_i} | i = 1, \dots, p+1\}$ be the $p+1$ subgroups of E of order p . One of the them is the kernel of the reduction map $E \rightarrow \tilde{E}$ over \mathbb{F}_p , let it be C_{p_0} , then the kernel of the Frobenius map $\text{Fr}_p : E \rightarrow E^{(p)}$ is exactly C_{p_0} and so we have: $E^{(p)} \simeq E/C_{p_0}$ and similarly $C_N^{(p)} = C_N + C_{p_0}/C_{p_0}$.

On the other hand we can factorise the multiplication by p map as:

$$p : E \xrightarrow{\phi} E/C_{p_i} \xrightarrow{\psi} E$$

for every $i = 1, \dots, p + 1$. We know that ϕ is separable since the kernel is C_{p_0} , so that ψ is the Frobenius morphism, which means that $(E/C_{p_i})^{(p)} \simeq E$ and with a similar reasoning we have $(C_N + C_{p_i}/C_{p_i})^{(p)} \simeq C_N$. Now we can conclude since we have equalities:

$$(E/C_{p_0}, C_N + C_{p_0}/C_{p_0}) = \text{Fr}_p(E, C_N)$$

and

$$\sum_{i \neq 0} (E/C_{p_i}, C_N + C_{p_i}/C_{p_i}) = \widehat{\text{Fr}}_p(E, C_N)$$

which implies the Eichler-Shimura relation, from the definition of T_p .

As we mentioned before we will not go into the details of proving that the same congruence relation holds on $X_0(N)_{/\mathbb{F}_p}$. \square

1.4 The modular parametrisation

In this section we are going to explain how the operators we introduced in the last section can be defined on the space of cusp forms and state, without proof, some important theorems from the theory of modular forms.

The proofs of this section may be found in [[Kna92]].

Consider the Hecke operators T_p , for all p .

Fix a basis of $(E, C_N) = (\mathbb{C}/[1, \tau], [1/N, \tau])$ and of $(E/C_p, C_N + C_p/C_p) = (\mathbb{C}/[1, \tau'], [1/N, \tau'])$, then an integer matrix which satisfies $[1, \tau'] = M[1, \tau]$ and $[1/N, \tau'] = M[1/N, \tau]$ must lie in the set:

$$M(p, N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}) \mid ad - bc = p, (a, N) = 1 \text{ and } N|c \right\}$$

and viceversa.

Let $S_2(\Gamma_0(N))$ be the space of weight two cusp forms for $\Gamma_0(N)$, it seems natural to have:

Definition 1.12 (Hecke Operator). Let $\{\alpha_i\}$ be a collection of coset representatives of $\Gamma_0(N) \backslash M(nN)^1$.

We define

$$\begin{aligned} T_n : S_2(\Gamma_0(N)) &\longrightarrow S_2(\Gamma_0(N)) \\ f &\longmapsto \sum_i f \circ [\alpha_i] \end{aligned}$$

where $f \circ [\alpha_i](\tau) = \det(\alpha_i)(c\tau + d)^{-2} f(\alpha_i\tau)$, if $\alpha_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Let us now turn to the Atkin-Lehner operator w_N .

¹Notice that $\Gamma_0(N)$ has finite index in $M(p, N)$.

Definition 1.13. Let $\alpha_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$.

The *Fricke involution* w_N on the space of weight 2 cusp forms $S_2(\Gamma_0(N))$ is defined in the following way:

$$w_N : S_2(\Gamma_0(N)) \longrightarrow S_2(\Gamma_0(N)) \\ f \longmapsto f \circ [\alpha_N]$$

explicitly $w_N f(\tau) = f \circ [\alpha_N](\tau) = \frac{1}{(N\tau)^2} f\left(\frac{-1}{N\tau}\right)$.

Remark. w_N is an involution on the space of weight two cusp forms, i.e. $w_N^2 = \text{id}$. If we consider the $+$ and the $-$ eigenspaces of $S_2(\Gamma_0(N))$ for w_N we have a direct sum decomposition:

$$S_2(\Gamma_0(N))^+ \oplus S_2(\Gamma_0(N))^-.$$

Define the *L-function* of a cusp form as:

$$L(s, f) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

where $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ is the q -expansion of f at the cusp ∞ , then we have the following:

Theorem 1.14 (Hecke). Let $f \in S_2(\Gamma_0(N))$ be a cusp form in one of the eigenspaces $S_2^{\epsilon_N}(\Gamma_0(N))$ of w_N , where $\epsilon_N = \pm 1$. Then $L(s, f)$ is initially defined for $\text{Res} > 2$ and extends to be entire in s . Moreover, the function

$$\Lambda(s, f) = N^{s/2} (2\pi)^{-s} \Gamma(s) L(s, f),$$

satisfies a functional equation:

$$\Lambda(s, f) = -\epsilon_N \Lambda(2 - s, f). \quad (1.4)$$

We would now like to study a little further the structure of the space $S_2(\Gamma_0(N))$. From this analysis we will be able to single out a particular modular function f for $\Gamma_0(N)$, which, through the so-called 'Eichler-Shimura construction', will let us construct a map from the modular curve to an elliptic curve E_f , $\phi : X_0(N) \longrightarrow E_f$, that is very important for all the considerations in the next chapter. In fact, through this map, we will be able to 'transport structure' from $X_0(N)$ to E_f .

First of all let us define an inner product on the space of cusp forms:

Definition 1.15. The *Petersson inner product* on $S_2(\Gamma_0(N))$ is defined as:

$$\langle f, h \rangle = \int_{R_N} f(\tau) \overline{h(\tau)} \frac{d\rho d\sigma}{\sigma^2},$$

where $\tau = \rho + i\sigma$ and R_N is a fundamental domain for $\Gamma_0(N)$.

The Hecke operators T_p with $p \nmid N$, on the space of cusp forms $S_k(\Gamma_0(N))$ are self adjoint relative to the Petersson inner product. So it can be proved that, since the Hecke operators T_p , for $p \nmid N$, commute, $S_2(\Gamma_0(N))$ splits into the orthogonal sum of simultaneous eigenspaces for the operators T_p with $p \nmid N$.

An cusp form which is an eigenvector T_p , with $p \nmid N$, is called an *eigenform*; eigenforms in the same eigenspace are said to be *equivalent*.

Moreover, since the Hecke operators commute with each other for all p , in each space of equivalent eigenforms in the decomposition of $S_2(\Gamma_0(N))$ there will be at least one eigenvector of all the T_p , also with $p|N$. We have the following:

Theorem 1.16 (Hecke-Petersson). The whole space $S_2(\Gamma_0(N))$ of cusp forms is the orthogonal sum of the spaces of equivalent eigenforms. Each space of equivalent eigenforms has a member which is an eigenvector for all the T_p .

Moreover, such an eigenform f in $S_2(\Gamma_0(N))$ can be normalised so that its q -expansion $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ has $c_1 = 1$ and the L -function for f , $L(s, f)$, has an Euler product expansion:

$$L(s, f) = \prod_{p|N} \left[\frac{1}{1 - c_p p^{-s}} \right] \prod_{p \nmid N} \left[\frac{1}{1 - c_p p^{-s} + p^{1-2s}} \right] \quad (1.5)$$

convergent for $\text{Res} > 2$.

The problem now is that, since in general the Fricke involution w_N and the Hecke operators T_p for $p|N$ do not commute, we are not able to identify a correlation between L -functions which have an Euler product expansion and L -functions which satisfy a functional equation.

The problem turns out to be coming from some cusp form which 'come trivially from modular forms of a lower level $d|N$ '.

Let us be more precise. If $r_1 r_2 | N$ and if $f(\tau)$ is an eigenform for $\Gamma_0(N/r_1 r_2)$, then $f(r_2 \tau)$ is an eigenform for $\Gamma_0(N)$ with the same eigenvalues. Such an eigenform is called an *oldform*.

The eigenforms in the orthogonal complement of the space of oldforms are called *newforms*.

There is the important 'Multiplicity one theorem', which characterises newforms:

Theorem 1.17 (Atkin-Lehner). If $f \in S_2(\Gamma_0(N))$ is a newform, then its equivalence class is one-dimensional, i.e. consists of the multiples of f .

Let us analyse a consequence of this theorem.

The operators w_N and T_p for $p|N$ commute with the Hecke operators T_p for $p \nmid N$, so they send each equivalence class to itself. In the case of a newform f the equivalence class is $\mathbb{C}f$, so this means that we can find an eigenform

f for w_N and for all the T_p s, such that as a consequence of theorems (1.14) and (1.16), its L -function $L(s, f)$ has an Euler product expansion as in (1.5) and satisfies a functional equation as in (1.4).

Let us summarise these results in the following:

Theorem 1.18 (Hecke-Petersson, Atkin-Lehner). The space $S_2(\Gamma_0(N))$ of weight 2 cusp forms admits the following decomposition:

$$S_2(\Gamma_0(N)) = \bigoplus_{d|N} \bigoplus_{e|\frac{N}{d}} D_e S_2(\Gamma_0(d))^{\text{new}},$$

where $D_e : g(\tau) \mapsto g(e\tau)$ and

$$S_2(\Gamma_0(d))^{\text{new}} \simeq \bigoplus_{g_\lambda} \mathbb{C}g_\lambda$$

with g_λ a normalised eigenform for $\Gamma_0(d)$.

The g_λ are eigenvectors for the Hecke operators T_p for all p and for the Fricke involution w_N and the following holds:

1. $T_p f = c_p f$ for all p ,
2. $w_N f = \epsilon_N f$ with $\epsilon_N = \pm 1$.

Moreover the L -function $L(s, f)$ has an Euler product expansion as in (1.5) and satisfies a functional equation with sign $-\epsilon_N$ as in (1.4).

Now we turn to the Eichler-Shimura theory. The next theorem will predict us the existence of a normalized newform f for $S_2(\Gamma_0(N))$ to which we can associate an elliptic curve E_f with a map from the modular curve $X_0(N)$ to E_f , which satisfies:

$$L(s, f) = L(s, E).$$

Theorem 1.19 (Eichler-Shimura). Let $f(\tau) = \sum_{n=1}^{\infty} c_n \exp(2\pi i n \tau)$ be a newform in $S_2(\Gamma_0(N))$ normalized to have $c_1 = 1$, and suppose that all the c_n are in \mathbb{Z} . Then there exists a pair (E_f, ν) such that:

1. E_f is an elliptic curve defined over \mathbb{Q} .
2. E_f is a quotient of $\text{Jac}(X_0(N))$ by $(T_p - c_p \cdot \text{id})\text{Jac}$, for all p , so that T_p acts on E_f as multiplication by the integers c_p , for all p .
3. The differential $\sum c_n q^n dq/q$ associated to f is a nonzero multiple of $\nu^*(\omega)$, where ω is the invariant differential of E .
4. If

$$\Lambda_f = \left\{ \int_{\tau_0}^{\gamma(\tau_0)} f(\xi) d\xi \mid \gamma \in \Gamma_0(N) \right\}$$

then Λ_f is a lattice in \mathbb{C} , and E is isomorphic to \mathbb{C}/Λ_f over \mathbb{C} .

5. $L(E, s)$ coincides with $L(f, s)$, for almost all c_p .

Remark. Eichler-Shimura proved point 5. for Euler factors for $p \nmid N$. For the 'bad' factors at $p|N$ this follows from results of Langlands and Carayol.

If we compose the map ν in the Eichler-Shimura construction with the inclusion map of $X_0(N) \hookrightarrow \text{Jac}(X_0(N))$ we obtain map defined over \mathbb{Q} :

$$\phi : X_0(N) \longrightarrow E_f. \tag{1.6}$$

The map ϕ is called the *Modular parametrisation* of E_f .

Theorem 1.20. (Carayol) The integer N is the conductor of E_f .

From a theorem of Wiles we can deduce that the viceversa also holds over \mathbb{Q} :

Theorem 1.21 (Wiles, Taylor-Wiles, Breuil-Conrad-Diamond). Let E be an elliptic curve over \mathbb{Q} of conductor N . Then there exists a newform $f \in S_2(\Gamma_0(N))$ such that:

$$L(E, s) = L(E, f)$$

Furthermore, from results on the Tate's conjecture for abelian varieties proved by Faltings, it can be deduced that E is isogenous to the elliptic curve E_f obtained via the Eichler-Shimura construction.

1.5 Definition of a Heegner point on $X_0(N)$.

In this section we are going to introduce the key definition of a Heegner point, which will be an important tool in the proof of the theorem on the rank of an elliptic curve in the next chapter.

Heegner points on $Y_0(N)$, or more generally on $X_0(N)$, correspond to (generalised) modular pairs (E, C_N) , where E and E/C_N both have complex multiplication by the same order \mathcal{O} .

Let us be more precise. Consider a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$, of discriminant $-D$.

For simplicity assume that $D \neq 3, 4$, so that the ring of integers \mathcal{O}_K of K has unit group $\mathcal{O}_K^\times = \{\pm 1\}$.

Fix an integer N , such that every prime dividing N is split completely in K . This assumption, called the 'Heegner Hypothesis', guarantees the existence of a prime ideal \mathfrak{N} of \mathcal{O}_K such that $\mathcal{O}_K/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}$. We also have $\mathfrak{N}^{-1}/\mathcal{O}_K \simeq \mathbb{Z}/N\mathbb{Z}$.

Now consider an order \mathcal{O} of K of conductor² n prime to N . $\mathfrak{N}_n = \mathfrak{N} \cap \mathcal{O}$ is

²In this mémoire, we will only be considering orders of squarefree conductor n .

an invertible ideal in \mathcal{O} , with $\mathfrak{N}_n^{-1}/\mathcal{O} \simeq \mathbb{Z}/N\mathbb{Z}$.
 $(\mathbb{C}/\mathcal{O}, \mathfrak{N}_n^{-1})$ is a modular pair, since if $E = \mathbb{C}/\mathcal{O}$, then

$$\mathfrak{N}_n^{-1}\mathcal{O}/\mathcal{O} \subset N^{-1}\mathcal{O}/\mathcal{O} = E[N],$$

so that $\mathfrak{N}_n^{-1}/\mathcal{O}$ is a cyclic subgroup of E of order N .

Definition 1.22.

$$x_n := (\mathbb{C}/\mathcal{O}, \mathfrak{N}_n^{-1}/\mathcal{O}) \tag{1.7}$$

is a *Heegner point* on $X_0(N)$.

Remark. Equivalently, we can describe Heegner points x_n as isomorphism classes of couples of elliptic curves:

$$(\mathbb{C}/\mathcal{O}, \mathbb{C}/\mathfrak{N}_n^{-1}),$$

with $\ker(\mathbb{C}/\mathcal{O} \rightarrow \mathbb{C}/\mathfrak{N}_n^{-1}) = \mathfrak{N}_n^{-1}/\mathcal{O} \simeq \mathbb{Z}/N\mathbb{Z}$.

Proposition 1.23. The Heegner point x_n as defined in (1.7) lies in $X_0(N)(K_n)$, where K_n is the ring class field of K conductor n .

Proof. (Sketch) As we saw in theorem (0.25) $K(j(\mathbb{C}/\mathcal{O})) = K(j(\mathbb{C}/\mathfrak{N}_n^{-1})) = K_n$ is the ring class field of K of conductor n . Moreover we can deduce from the birational equivalence β of (1.2) that, outside a finite number of singular points of the modular equation, we can consider the point x_n on $X_0(N)$ as having coordinates $(j(\mathbb{C}/\mathfrak{N}_n^{-1}), j(\mathbb{C}/\mathcal{O}))$. So we deduce that

$$x_n \in X_0(N)(K_n).$$

For what concerns those finite number of singular points for the modular equation, the proof is a little more complicated so we will not go into the details here. \square

We recall that K_n is a normal extension of \mathbb{Q} and the Galois group $\text{Gal}(K_n/\mathbb{Q})$ is the semi-direct product of its normal subgroup $\text{Gal}(K_n/K)$, isomorphic to $\text{Pic}(\mathcal{O})$ by (0.11), and the group $\text{Gal}(K/\mathbb{Q})$ of order 2, generated by complex conjugation τ , which acts on $\text{Gal}(K_n/K) \simeq \text{Pic}(\mathcal{O})$ by sending an ideal \mathfrak{a} to its inverse $\mathfrak{a}^{-1} = \tau\mathfrak{a}\tau^{-1}$.

Heegner points of conductor n are stable under the action of $\text{Gal}(K_n/\mathbb{Q})$.

Proposition 1.24. The action of complex conjugation $\tau \in \text{Gal}(K_n/\mathbb{Q})$ is as following:

$$\tau x_n = \tau((\mathbb{C}/\mathcal{O}, \mathfrak{N}_n^{-1}/\mathcal{O})) = (\mathbb{C}/\mathcal{O}, \overline{\mathfrak{N}_n^{-1}}/\mathcal{O}) = (\mathbb{C}/\mathcal{O}, \mathfrak{N}_n N^{-1}\mathcal{O}/\mathcal{O}).$$

Moreover, directly from the theory of complex multiplication, theorem (0.25), we have the following:

Proposition 1.25. Let $\sigma \in \text{Gal}(K_n/K)$. Then we have:

$$\sigma x_n = \sigma(\mathbb{C}/\mathcal{O}, \mathfrak{N}_n^{-1}/\mathcal{O}) = (\mathbb{C}/\mathfrak{a}_\sigma^{-1}, \mathfrak{N}_n^{-1}\mathfrak{a}_\sigma^{-1}/\mathcal{O}),$$

where $\mathfrak{a}_\sigma \in \text{Pic}\mathcal{O}$ is the ideal class that corresponds to σ under the isomorphism of theorem (0.11).

Proof. We have seen in theorem (0.26), that $\sigma \in \text{Gal}(K_n/K)$ acts on j -invariants by sending $j(-)$ to $j(- \cdot \mathfrak{a}_\sigma^{-1})$. In the present case we have that:

$$\sigma(j(\mathcal{O}), j(\mathfrak{N}_n^{-1})) = (j(\mathcal{O} \cdot \mathfrak{a}_\sigma^{-1}), j(\mathfrak{N}_n^{-1} \cdot \mathfrak{a}_\sigma^{-1})),$$

so that $\sigma(\mathbb{C}/\mathcal{O}, \mathfrak{N}_n^{-1}/\mathcal{O}) = (\mathbb{C}/\mathfrak{a}_\sigma^{-1}, (\mathfrak{N}_n\mathfrak{a}_\sigma/\mathcal{O})^{-1})$. \square

The Heegner points of conductor n are also stable under the action of the Atkin-Lehner involutions and the Hecke operators T_p , for $p \nmid N$.

The Atkin-Lehner involution w_N acts on Heegner points via the formula:

$$w_N((\mathbb{C}/\mathcal{O}, \mathfrak{N}_n^{-1}/\mathcal{O})) = (\mathbb{C}/\mathfrak{N}_n^{-1}, N^{-1}\mathcal{O}/\mathfrak{N}_n^{-1}).$$

from which we can deduce that:

$$w_N^2(x_n) = w_N(\mathbb{C}/\mathfrak{N}_n^{-1}, N^{-1}\mathcal{O}/\mathfrak{N}_n^{-1}) = (\mathbb{C}/N^{-1}\mathcal{O}, \mathfrak{N}_n^{-1}\mathcal{O}/N^{-1}\mathcal{O}) \simeq x_n,$$

where the last isomorphism is given by the isomorphism multiplication by $N : \mathbb{C}/N^{-1}\mathcal{O} \xrightarrow{\sim} \mathbb{C}/\mathcal{O}$.

Let $n = ml$, l prime which does not divide m , we have the following diagram:

$$\begin{array}{ccccc}
 & & K_n & & \\
 & G_m & \swarrow & \searrow & G_l \\
 K_l & & & & K_m \\
 & \searrow & & \swarrow & \\
 & & K_1 & & \\
 & & | & & \\
 & & K & & \\
 & & | & & \\
 & & \mathbb{Q} & &
 \end{array} \tag{1.8}$$

Call $G_n = \text{Gal}(K_n/K_1)$ the Galois group of the extension K_n/K_1 . Since $\mathcal{O}_K^\times = \mathbb{Z}^\times = \{\pm 1\}$, K_l and K_m are disjoint and so we have:

$$G_n \simeq \prod_{l|n} G_l = G_l \times G_m,$$

where $G_l = \text{Gal}(K_n/K_m)$.

Moreover we have an exact sequence:

$$0 \rightarrow \text{Gal}(K_l/K_1) \rightarrow G_n \rightarrow G_m \rightarrow 0,$$

then we deduce from example (0.21):

$$G_l \simeq \text{Gal}(K_n/K_1) \simeq \mathbb{F}_\lambda^\times / \mathbb{F}_l^\times.$$

Now let us assume that λ is inert in K , then $\mathbb{F}_\lambda^\times \simeq \mathbb{F}_{l^2}^\times$, so that G_l is cyclic of order $l + 1$.

Let us now consider a trace map, which we define on the Jacobian of the modular curve $\text{Tr}_l : J(X_0(N))(K_n) \rightarrow J(X_0(N))(K_m)$ which sends

$$x \mapsto \sum_{\sigma \in G_l} \sigma x.$$

Proposition 1.26. With the above notation and hypothesis we have:

$$T_l(x_m) = \text{Tr}_l(x_n),$$

where T_l is the Hecke operator on $J(X_0(N))$.

Proof. Let $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ be the order of conductor n in K . Call $\mathbb{C} = \mathbb{C}/\mathcal{O}_n$ and $C_N = \mathfrak{N}_n^{-1}/\mathcal{O}_n$. By definition we have:

$$T_l(x_n) = \sum_{C_l \subset E[l]} (E/C_l, C_N + C_l/C_l),$$

where the sum is over the $l + 1$ cyclic subgroups of $E[l]$ of order l .

On the other hand, since $(l, m) = 1$, we have

$$x_n = (E, C_N) = (\mathbb{C}/\mathcal{O}_n, \mathfrak{N}_n^{-1}/\mathcal{O}_n) = ((\mathbb{C}/\mathcal{O}_m)/C_l, (\mathfrak{N}_n^{-1}/\mathcal{O}_m)/C_l)$$

for some unique cyclic subgroup of order l C_l , since $\mathcal{O}_m/\mathcal{O}_n$ is cyclic of order l . Furthermore

$$\begin{aligned} \text{Tr}_l(x_m) &= \sum_{\sigma \in G_l} \sigma x_n \\ &= \sigma(\mathbb{C}/\mathcal{O}_n, \mathfrak{N}_n^{-1}/\mathcal{O}_n) \\ &= \sigma((\mathbb{C}/\mathcal{O}_m)/C_l, (\mathfrak{N}_n^{-1}/\mathcal{O}_m)/C_l) \\ &= ((\mathbb{C}/\mathcal{O}_m)/\mathfrak{a}_\sigma C_l, (\mathfrak{N}_n^{-1}/\mathcal{O}_m)/\mathfrak{a}_\sigma C_l), \end{aligned} \tag{1.9}$$

where $\mathfrak{a}_\sigma C_l$ is another cyclic subgroup of order l of \mathbb{C}/\mathcal{O}_n . Indeed, since $\sigma \in G_l = \text{Gal}(K_n/K_m)$, then $\mathfrak{a}_\sigma \mathcal{O}_m$ is principal and so $\mathfrak{a}_\sigma(\mathcal{O}_m/\mathcal{O}_n) \simeq \mathfrak{a}_\sigma C_l$ is another cyclic subgroup of order l .

So we are done. \square

1.6 Heegner points on elliptic curves

Let E be an elliptic curve over \mathbb{Q} of conductor N . Fix a modular parametrisation defined over \mathbb{Q} :

$$\phi : X_0(N) \longrightarrow E$$

By means of this parametrisation we can transport the Heegner point construction from the modular curve to the elliptic curve, so that we can obtain certain points on E defined over ring class fields.

Define

$$y_n := \phi(x_n) \in E(K_n), \tag{1.10}$$

where K_n is the ring class field of K of conductor n .

Furthermore if we let $x_1 := (\mathbb{C}/\mathcal{O}_K, \mathfrak{N}^{-1}/\mathcal{O}_K) \in X_0(N)(K_1)$, where K_1 is the Hilbert class field of K , then define

$$y_1 = \phi(x_1) \in E(K_1)$$

and

$$y_K = \mathrm{Tr}_{K_1/K}(y_1) \in E(K), \tag{1.11}$$

where the trace is taken by summing the conjugates of y_1 using the group law on E .

Chapter 2

Kolyvagin's Theorem

In this chapter we are going to prove the main result of this 'mémoire', which is proposition (2.2). First of all, given an elliptic curve E over \mathbb{Q} we are going to use Heegner points to show the construction of a system of cohomology classes in the Galois cohomology of E , section (2.4), and study their properties. Then, using some results from Tate's local duality and some Galois cohomology computations, we will be able to bound the order of the p -Selmer group of E/K and finally deduce our result.

In the late 80's Kolyvagin published a paper in which he used Birch's construction of a Heegner point to define a system of Heegner points, which satisfied the properties of what is now called an Euler system, and used this construction to prove the following theorem:

Theorem 2.1. Let E be an elliptic curve over \mathbb{Q} .

Assume that the point y_K , as defined in (1.11), has infinite order in $E(K)$.

Then:

1. the group $E(K)$ has rank 1.
2. the group $\text{III}(E/K)$ is finite.

In his paper [Gr84] Gross does not prove all of this result, but explains the proof of a slightly weaker proposition to illustrate Kolyvagin's main argument:

Theorem 2.2. Let p be an odd prime such that the extension $\mathbb{Q}(E_p)/\mathbb{Q}$ has Galois group $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{\text{tors}}$. Then:

1. The group $E(K)$ has rank 1.
2. The p -torsion subgroup of $\text{III}(E/K)$ is trivial.

Remark. These assumptions make sense, in fact if E does not have complex multiplication then $\mathbb{Q}(E_p)$, the field generated over \mathbb{Q} by the p -division

points of E , has Galois group over \mathbb{Q} isomorphic to $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for all sufficiently large primes p .

Moreover modulo torsion we can always find a p which does not divide y_K , since thanks to the Mordell-Weil theorem y_K is not ‘infinitely divisible’ in $E(K)/E(K)_{\mathrm{tors}}$. In fact, since the group $E(K)$ is finitely generated, there exists only a finite number of integers $n \in \mathbb{N}$ such that $y_K = nP$, where $P \in E(K) \setminus E(K)_{\mathrm{tors}}$.

We know, from (0.5), that there exists a sequence of \mathbb{F}_p -vector spaces:

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} \mathrm{Sel}_p(E/K) \longrightarrow \mathrm{III}(E/K)_p \longrightarrow 0,$$

From the hypothesis of theorem (2.2), we can deduce that $E(K)$ contains no p -torsion so we have:

$$r(E/K) = \dim_{\mathbb{F}_p} E(K)/pE(K), \quad (2.1)$$

which means that we are left to proving:

Proposition 2.3. Let p be an odd prime such that the extension $\mathbb{Q}(E_p)/\mathbb{Q}$ has Galois group isomorphic to $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)$ modulo $E(K)_{\mathrm{tors}}$. Then the group $\mathrm{Sel}_p(E/K)$ is cyclic generated by $\delta(y_K)$.

Let us see how this proposition implies the result in (2.2).

Indeed if $0 \neq y_K \in E(K)/pE(K)$, then $\dim_{\mathbb{F}_p}(E(K)/pE(K)) \neq 0$, but $E(K)/pE(K)$ injects into $\mathrm{Sel}_p(E/K)$, which has rank one by proposition (2.3) and so by (2.1) $r(E/K) = 1$. So we have 1.

Moreover $\delta : E(K)/pE(K) \rightarrow \mathrm{Sel}_p(E/K)$ is an isomorphism of \mathbb{F}_p -vector spaces so the cokernel, which equals $\mathrm{III}(E/K)_p$, is zero. So we have 2.

In the rest of the chapter we are going to illustrate a proof of this proposition.

Let us set some notation. E is an elliptic curve over \mathbb{Q} of conductor N .

K is an imaginary quadratic field with discriminant $-D \neq 2, 3$, which satisfies the Heegner condition, i.e. every prime dividing N is split completely in K .

Furthermore we make the assumption that all the Heegner points we consider have conductor n , which satisfies the following hypothesis:

$$n \text{ is squarefree and for all } l|n, l \text{ does not divide } N \cdot D \cdot p. \quad (2.2)$$

2.1 Galois action on torsion points

Let $K(E_p)$ the Galois extension obtained by adjoining to K the coordinates of the p -torsion points of E .

In this section we are going to consider the p -torsion points on E , for p prime, and see how the Galois group $\text{Gal}(K(E_p)/\mathbb{Q})$ acts on them.

Proposition 2.4. The extension $K(E_p)/K$ is unramified outside the primes which divide $p \cdot N$.

Proof. Let λ be a prime of K which does not lie above pN . E has good reduction over \mathcal{O}_{K_λ} , so if γ is a prime lying above λ it is enough to show that the extension of the residue fields $\mathbb{F}_\gamma/\mathbb{F}_\lambda$ has the same degree as $K(E_p)_\gamma/K_\lambda$. The curve reduction of E over \mathbb{F}_λ is an elliptic curve \tilde{E} and so from (0.9) we deduce that the reduction map gives an injection:

$$E_p \hookrightarrow \tilde{E}(\mathbb{F}_\gamma).$$

An element of the inertia group of $K(E_p)_\gamma/K_\lambda$ then fixes all elements of $K(E_p)_\gamma$ since it fixes their images in \mathbb{F}_γ , so it is trivial. Then we are done since the index of ramification e equals the order of the inertia subgroup. \square

Remark. It follows from the last proposition that every prime l which divides integers satisfying (2.2) is unramified in $K(E_p)/\mathbb{Q}$.

We denote by $\text{Frob}(l)$ the conjugacy class in $\text{Gal}(K(E_p)/\mathbb{Q})$ containing the generators of $\text{Gal}(\mathbb{F}_\gamma/\mathbb{F}_l)$ for every prime γ above l .

We assume that:

$$\tau \in \text{Frob}(l), \tag{2.3}$$

where τ is complex conjugation.

One often says that l satisfying (2.3) is a 'Kolyvagin prime'.

Remark. By Chebotarev density theorem, theorem (0.22), there is an infinite number Kolyvagin primes.

As a consequence of (2.3) we have that l remains inert in K ; call λ its unique prime factor in K .

Proposition 2.5. Assumption (2.3) implies that

$$a_l \equiv l + 1 \equiv 0 \pmod{p},$$

where $l + 1 - a_l = |\tilde{E}(\mathbb{F}_l)|$

Proof. It follows directly from the computations of the characteristic polynomials of the Frobenius automorphisms acting on E_p . In fact complex conjugation satisfies $x^2 - 1 \equiv 0 \pmod{p}$, while $\text{Frob}(l)$ is such that $\text{Frob}(l)^2 - a_l \text{Frob}(l) + l \equiv 0 \pmod{p}$, with $l + 1 - a_l = |\tilde{E}(\mathbb{F}_l)|$. So from (2.3) we deduce that:

$$x^2 - a_l x + l \equiv x^2 - 1 \pmod{p},$$

which implies $a_l \equiv l + 1 \equiv 0 \pmod{p}$. \square

Remark. Recall that the a_l s in proposition (2.5) are the coefficients of the L -function of E as defined in (0.14), which coincide with the coefficients of the L -function of f , the newform associated to E .

Let \mathbb{F}_l denote the residue field at λ , which has l^2 elements. By (2.3) the prime λ splits completely in $K(E_p)/K$, which implies that the residue field at a prime λ_i of $\mathcal{O}_{K(E_p)}$ above λ is the same as \mathbb{F}_λ , i.e. $\mathbb{F}_{\lambda_i} \simeq \mathbb{F}_\lambda$. Moreover

$$\tilde{E}(\mathbb{F}_\lambda)_p \simeq \tilde{E}(\mathbb{F}_{\lambda_i})_p \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

We can now consider the action of complex conjugation on this space and deduce:

Proposition 2.6. There exists the following decomposition into eigenspaces for complex conjugation of the reduction of the torsion points in the residue field \mathbb{F}_λ :

$$\tilde{E}(\mathbb{F}_\lambda)_p^\pm \simeq \mathbb{Z}/p\mathbb{Z},$$

where \cdot^+ is the plus eigenspace of the automorphism group $\{1, \tau\}$ and \cdot^- is the minus one.

Proof. If we call Fr_l the Frobenius map $x \mapsto x^l$ we know that $\text{Fr}_l = \tau$ on \mathbb{F}_λ . So that:

$$|\tilde{E}(\mathbb{F}_\lambda)_p^+| = |\{P \in E_p | \text{Fr}_l P = P\}| = |\tilde{E}(\mathbb{F}_l)_p| = |l + 1 - a_l| \equiv 0 \pmod{p}$$

$$\begin{aligned} |\tilde{E}(\mathbb{F}_\lambda)_p^-| &= |\{P \in E_p | \text{Fr}_l P = -P\}| = |\ker(\text{Fr}_l + 1)| \equiv \deg(\text{Fr}_l + 1) \\ &\equiv \det(\text{Fr}_l + 1) \equiv \text{Tr}(\text{Fr}_l) + \det(\text{Fr}_l) + 1 \equiv a_l + l + 1 \equiv 0 \pmod{p} \end{aligned}$$

□

2.2 Construction of an 'Euler system'

Consider the collection of Heegner points of conductor n that we defined in section (2.4). Recall that the integer n is assumed to satisfy (2.2) and every $l|n$ is assumed to be a Kolyvagin prime, (2.3).

Recall from section (??) that we have $G_n = \text{Gal}(K_n/K_1) \simeq \prod_{l|n} G_l = G_l \times G_m$, where $G_l = \text{Gal}(K_n/K_m)$.

Moreover from example (0.21) and the fact that $\lambda = l\mathcal{O}_K$ is inert in K we deduce that:

$$G_l \simeq \text{Gal}(K_n/K_1) \simeq \mathbb{F}_\lambda^\times / \mathbb{F}_l^\times \simeq \mathbb{F}_{l^2}^\times / \mathbb{F}_l^\times,$$

which is cyclic of order $l + 1$.

We can now prove the 'Euler system' properties that are satisfied by the system of Heegner points $y_n \in E(K_n)$:

- Proposition 2.7.** 1. $\text{Tr}_l y_n = a_l \cdot y_m \in E(K_m)$,
2. Each prime factor λ_n of l in K_n divides a unique prime $\lambda_m \in K_m$ and we have the congruence $y_n \equiv \text{Frob}(\lambda_m)y_m \pmod{\lambda_n}$.

Proof. 1. This follows from lemma (??) and the fact that the Hecke operator T_l acts on the points of the elliptic curve as multiplication by the coefficients a_l , cf. theorem (1.19, 2.). So we have:

$$\text{Tr}_l y_m = \text{Tr}_l \phi(x_m) = \phi(\text{Tr}_l x_m) = \phi(T_l x_m), = a_l \phi(x_m) = a_l \cdot y_m$$

where ϕ is the modular parametrisation.

2. We are going to prove the corresponding fact on $X_0(N)$:

$$x_n \equiv \text{Frob}(\lambda_m)x_m \text{ in } \mathbb{F}_{\lambda_n}$$

and then conclude using the modular parametrisation.

Indeed, the prime λ is principal in K and has norm prime to m , so it is in the kernel of the Artin map (0.10), which means that it is split completely in K_m/K .

The factors λ_m of λ in K_m are totally ramified in K_n , i.e.

$$\lambda_m = (\lambda_n)^{l+1},$$

this follows from the fact that since $\mathcal{O}_K^\times = \{\pm 1\}$ only the primes dividing the conductor are ramified. So In particular the residue fields coincide:

$$\mathbb{F}_{\lambda_m} = \mathbb{F}_{\lambda_n} = \mathbb{F}_\lambda = \mathbb{F}_{l^2}$$

Now consider $T_l(x_m) = \text{Tr}_l(x_n)$. The points in this divisor are conjugates of x_n over K_m , so they are all congruent to x_n , modulo λ_n . The Eichler-Shimura congruence relation (1.11) $T_l = \text{Fr}_l + \hat{\text{Fr}}_l \pmod{l}$ shows that one, and hence all, elements are congruent to $\text{Frob}(\lambda_m)x_m$ and we deduce:

$$\text{Frob}(\lambda_m)x_m \equiv x_n \pmod{\lambda_n}$$

□

2.3 Construction of cohomology classes.

In this section we are going to use the system of Heegner points we have just defined to construct cohomology classes in $H^1(K, E_p)$. One way to do so would be to simply take the trace of the points y_n from K_n to K and then push it to $H^1(K, E_p)$ through the map δ , but this does not yield interesting information. Instead we shall apply an operator to the y_n in order to obtain $\text{Gal}(K_n/K_1)$ -invariant elements, then computing the trace from K_1 to K will yield the desired $\text{Gal}(K_n/K)$ -invariant classes.

Let σ_l be a fixed generator of $G_l = \text{Gal}(K_n/K_1)$, cyclic subgroup of order $l + 1$ of $G_n = \text{Gal}(K_n/K_1)$.

The augmentation ideal of the group ring $\mathbb{Z}[G_l]$, i.e. the kernel of the map $\sum_{\sigma \in G_l} n_i \sigma^i \mapsto \sum n_i$, is principal and generated by $\sigma_l - 1$. Let

$$\text{Tr}_l := \sum_{\sigma \in G_l} \sigma \in \mathbb{Z}[G_l]$$

and let D_l be a solution of the following equation in $\mathbb{Z}[G_l]$:

$$(\sigma_l - 1) \cdot D_l = l + 1 - \text{Tr}_l.$$

Remark. 1. A solution exists, for example Kolyvagin takes

$$D_l = \sum_{i=1}^l i \cdot \sigma_i = - \sum_{i=1}^{l+1} \frac{\sigma_l^i - 1}{\sigma_l - 1}.$$

2. D_l is well defined up to addition of elements in the subgroup $\mathbb{Z}\text{Tr}_l$.

Let $D_n = \prod D_l$ in $\mathbb{Z}[G_n]$.

Proposition 2.8. The point $D_n y_n \in E(K_n)$ gives a class $[D_n y_n] \in E(K_n)/pE(K_n)$ which is fixed by G_n .

Proof. It suffices to show that for all $l|n$ $[D_n y_n]$ is fixed by σ_l the generator of G_l . Hence we must prove that: $(\sigma_l - 1)D_n y_n \in pE(K_n)$.

$$\begin{aligned} (\sigma_l - 1)D_n &= (\sigma_l - 1)D_l D_m = (l + 1 - \text{Tr}_l)D_m \in \mathbb{Z}[G_n], \\ &\Rightarrow (\sigma_l - 1)D_n y_n = (l + 1)D_m y_n - D_m(\text{Tr}_l y_n) \end{aligned}$$

since $l + 1 \equiv 0 \pmod{p}$ (congruence (2.5)), it now suffices to show that $\text{Tr}_l y_n \in pE(K_m)$. This follows from the congruence $a_l \equiv 0 \pmod{p}$ (2.5) and part 1 of proposition (2.7). \square

We would like to construct a point in $E(K_n)/pE(K_n)$ which is invariant not only for $G_n = \text{Gal}(K_n/K_1)$ but also for $\mathcal{G}_n := \text{Gal}(K_n/K)$.

To do so, consider a set S of coset representatives for the subgroup G_n in \mathcal{G}_n and define:

$$P_n := \sum_{\sigma \in S} \sigma D_n y_n.$$

Then clearly the class $[P_n]$ is in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$.

In order to define a system of cohomology classes we first need a lemma:

Lemma 2.9. The curve E has no p -torsion rational over K_n .

Proof. If not, either $E_p(K_n) = \mathbb{Z}/p\mathbb{Z}$ or $E_p(K_n) = (\mathbb{Z}/p\mathbb{Z})^2$. The first implies that E_p has a cyclic subgroup scheme over \mathbb{Q} , as K_n is Galois over \mathbb{Q} . Hence the Galois group of $\mathbb{Q}(E_p)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. If $E(K_n)_p = (\mathbb{Z}/p\mathbb{Z})^2$, then $Q(E_p)$ is a subfield of K_n and we have a surjective homomorphism $\mathcal{G}_n \rightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. This is impossible whenever $p > 2$. \square

From this lemma it follows immediately:

Proposition 2.10. There exists an isomorphism induced by restriction:

$$\mathrm{H}^1(K, E_p) \xrightarrow{\sim} \mathrm{H}^1(K_n, E_p)^{\mathcal{G}_n}.$$

Proof. From the terms of low degree of the Hochschild-Serre spectral sequence we have:

$$0 \rightarrow \mathrm{H}^1(\mathcal{G}_n, E(K_n)_p) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(K, E_p) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(K_n, E_p)^{\mathcal{G}_n} \rightarrow \mathrm{H}^2(\mathcal{G}_n, E(K_n)_p),$$

where the last arrow is transgression.

From lemma (2.9) we deduce that $E(K_n)_p = 0$, so the kernel of the map Res is 0, while the cokernel injects into a group which is 0. So it is an isomorphism. \square

Let us now define the cohomology classes.

Consider the following diagram:

$$\begin{array}{ccccccc}
& & & & & 0 & \\
& & & & & \downarrow & \\
& & & & & \mathrm{H}^1(K_n/K, E(K_n))_p & \\
& & & & & \downarrow \mathrm{Inf} & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & \mathrm{H}^1(K, E_p) & \longrightarrow & \mathrm{H}^1(K, E)_p \longrightarrow 0 \\
& & \downarrow & & \sim \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & \mathrm{H}^1(K_n, E_p)^{\mathcal{G}_n} & \longrightarrow & \mathrm{H}^1(K_n, E)_p^{\mathcal{G}_n}
\end{array} \tag{2.4}$$

The two rows are exact, by diagram (0.4). The column on the right is the inflation-restriction sequence for $\mathrm{Gal}(K_n/K) \leq \mathrm{Gal}(\overline{K}/K)$ and the middle vertical map is an isomorphism from proposition (2.10).

Let $c(n)$ be the unique class in $\mathrm{H}^1(K, E_p)$ such that:

$$\mathrm{Res} c(n) = \delta_n [P_n] \text{ in } \mathrm{H}^1(K_n, E_p)^{\mathcal{G}_n}. \tag{2.5}$$

Let

$$d(n) = \mathrm{Im} c(n) \text{ in } \mathrm{H}^1(K, E)_p. \tag{2.6}$$

By easy commutativity of the diagram and exactness of the bottom row, $\text{Res } d(n) = 0$. So there exists a unique $\widetilde{d}(n) \in H^1(K_n/K, E(K_n))_p$ such that

$$\text{Inf } \widetilde{d}(n) = d(n) \text{ in } H^1(K, E)_p \quad (2.7)$$

Directly from the construction we deduce the following:

Proposition 2.11. 1. The class $c(n) \in H^1(K, E_p)$ is trivial if and only if $P_n \in pE(K_n)$.
2. The class $d(n) \in H^1(K, E)_p$ and $\widetilde{d}(n) \in H^1(K_n/K, E)_p$ are trivial if and only if $P_n \in pE(K_n) + E(K)$.

Proof. 1. The class $c(n)$ is trivial if and only if $\delta_n(P_n)$ is trivial, but since δ_n is injective we have

$$\delta_n(P_n) = 0 \Leftrightarrow P_n = 0 \text{ in } (E(K_n)/pE(K_n))^{\mathcal{G}_n} \Leftrightarrow P_n \in pE(K_n).$$

2. Since Inf is injective we have:

$$d(n) = 0 \Leftrightarrow \widetilde{d}(n) = 0$$

and this happens if and only if either $c(n)$ is trivial, (condition 1.), or $c(n)$ is in the image by δ of an element in $E(K)/pE(K)$. \square

The cohomology classes we have just constructed are represented by explicit 1-cocycles:

$$\begin{aligned} c(n) : \text{Gal}(\overline{K}/K) &\longrightarrow E_p \\ \sigma &\longmapsto f(\sigma) := \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n - \frac{(\sigma-1)P_n}{p} \end{aligned}$$

and

$$\begin{aligned} \widetilde{d}(n) : \mathcal{G}_n = \text{Gal}(K_n/K) &\longrightarrow E_p \\ \sigma &\longmapsto \widetilde{f}(\sigma) := -\frac{(\sigma-1)P_n}{p} \end{aligned}$$

2.4 Properties of the cohomology classes $c(n)$.

In this section we would like to investigate on the properties of the cohomology classes we have just constructed.

First of all we shall see how they behave under the action of complex conjugation.

Since p is odd we know we have a direct sum decomposition:

$$H^1(K, E_p) \simeq H^1(K, E_p)^+ \oplus H^1(K, E_p)^-$$

Recall from proposition (1.18) that the eigenform $f = \sum a_n q^n$ associated to the elliptic curve E satisfies: $f(w_N z) = \epsilon \cdot f(z)$, where $-\epsilon$ is the sign of the functional equation which is satisfied by the L-function associated to E over \mathbb{Q} .

Proposition 2.12. We have

$$\tau x_n = w_N(\sigma x_n),$$

which implies

$$\tau y_n = \epsilon \sigma y_n + (\text{torsion}).$$

Proof. The first relation follows immediately from the definitions in section (1.5). So we have:

$$\tau(x_n - \infty) = w_N \sigma(x - \infty) + (w_N \infty - \infty).$$

for some $\sigma \in \mathcal{G}_n$ and we can conclude by the relation

$$\phi(w_N \sigma'(x_n - \infty)) = \epsilon \phi(\sigma y_n)$$

and by Manin-Drinfeld theorem which implies that the class $(0 - \infty)$ is torsion in the Jacobian $J(X_0(N))$ and so in E . □

Proposition 2.13. 1. The class $[P_n]$ lies in the $\epsilon_n = \epsilon \cdot (-1)^{f_n}$ eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$, where $f_n = |\{l : l|n\}|$.

2. The class $c(n)$ lies in the ϵ_n -eigenspace for τ in $H^1(K, E_p)$ and the class $d(n)$ lies in the ϵ_n -eigenspace for τ in $H^1(K, E)_p$.

Proof. 1. The lift of complex conjugation $\tau \in \text{Gal}(K_n/\mathbb{Q})$ acts on elements $\sigma \in \mathcal{G}_n$ by sending $\tau^{-1}\sigma\tau$ to the inverse σ^{-1} , so we have the commutation relation:

$$\tau\sigma = \sigma^{-1}\tau.$$

Now consider the action of τ on P_n :

$$\tau P_n = \tau \sum_{\sigma \in S} \sigma D_n y_n = \sum_{\sigma \in S} \sigma^{-1} \tau D_n y_n,$$

where $D_n = \prod_{l|n} D_l$, with D_l such that $(\sigma_l - 1)D_l = l + 1 - \text{Tr}_l$.

Considering the fact that:

$$(l + 1 - \text{Tr}_l)\tau = (l + 1)\tau - \sum_{\sigma \in G_l} \sigma\tau = \tau(l + 1) - \tau \sum_{\sigma \in G_l} \sigma^{-1} = \tau(l + 1 - \text{Tr}_l)$$

we have

$$(\sigma_l - 1)D_l\tau = \tau(\sigma_l - 1)D_l = -\sigma_l^{-1}(\sigma_l - 1)\tau D_l,$$

so that:

$$(\sigma_l - 1)(\sigma_l D_l \tau + \tau D_l) = 0$$

which means, by direct computation, that $\sigma_l D_l \tau + \tau D_l = k \text{Tr}_l$ for some $l \in \mathbb{Z}$.

Since $\text{Tr}_l y_n = a_l y_m \equiv 0 \pmod{pE(K_n)}$ then

$$\begin{aligned} \tau P_n &= \sum_{\sigma \in S} \sigma^{-1} \prod_{l|n} (\tau D_l) y_n \equiv \sum_{\sigma \in S} \sigma^{-1} \prod_{l|n} (-\sigma_l D_l \tau) y_n \\ &\equiv (-1)^{f_n} \left(\prod_{l|n} \sigma_l \right) \sum_{\sigma \in S} \sigma^{-1} D_n (\tau y_n) \pmod{pE(K_n)} \end{aligned}$$

But $\tau y_n = \epsilon \sigma' y_n + (\text{torsion})$, by proposition (2.12), for some $\sigma' \in \mathcal{G}_n$ and lemma (2.9) shows that $E(K_n)_p = 0$. Hence:

$$\tau P_n \equiv \epsilon_n \prod_{l|n} \sigma_l \sigma' \cdot \sum_{\sigma \in S} \sigma^{-1} D_n y_n \pmod{pE(K_n)}$$

But $\prod_{l|n} \sigma_l \sigma' \in \mathcal{G}_n$ and $\sum_{\sigma \in S} \sigma^{-1} D_n y_n = P_n$ which is invariant under the action of \mathcal{G}_n modulo $pE(K_n)$, so:

$$\tau P_n \equiv \epsilon_n P_n \pmod{pE(K_n)}$$

and 1. is proved.

2. clearly follows from 1. and the fact that the action of complex conjugation τ commutes with the maps in diagram (2.4). \square

2.5 Local triviality of the cohomology classes.

In this section we would like to decide if the classes $c(n)$ we have constructed lie in the p -Selmer group as defined in (0.3).

Let us recall diagram (0.4):

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{f} & H^1(K, E)_p \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow g \\ 0 & \longrightarrow & E(K_v)/pE(K_v) & \longrightarrow & H^1(K_v, E_p) & \longrightarrow & H^1(K_v, E)_p \longrightarrow 0 \end{array} \quad (2.8)$$

Now $c(n) \in H^1(K, E_p)$ is in the p -Selmer group ($= \ker(g \circ f)$) if and only if the reduction $d(n)_v \in H^1(K_v, E)_p$ of $f(c(n)) = d(n) \in H^1(K, E)_p$ is trivial at every prime v .

Proposition 2.14. The class $d(n)_v$ is locally trivial in $H^1(K_v, E)_p$ at the archimedean prime $v = \infty$ and at all the finite primes v of K which do not divide n .

Proof. If $v = \infty$ then $K_\infty = \mathbb{C}$, since K is imaginary quadratic, and Galois cohomology of E is trivial ($H^1(\mathbb{C}, E) = 0$).

Case 1. $(v, n \cdot N) = 1$.

$d(n)$ is inflated from a class $\tilde{d}(n) \in H^1(K_n/K, E(K_n))_p$, definition (2.7), where K_n/K is unramified at v . Hence $d(n)_v$ lies in the image of the subgroup $H^1(K_v^{\text{ur}}/K_v, E)_p$, where K_v^{ur} is the maximal unramified extension. We are going to prove that this group is trivial when E has good reduction at v .

In fact, let q be the prime of \mathbb{Z} which lies under v , recall that we have an exact sequence, sequence (0.7):

$$0 \rightarrow E_1 \rightarrow E \rightarrow \tilde{E} \rightarrow 0,$$

where E_1 is a pro- q group.

Then we can deduce that $H^1(K_v^{\text{ur}}/K_v, E_1)_p = 0$ and so there is an injection:

$$H^1(K_v^{\text{ur}}/K_v, E)_p \hookrightarrow H^1(\mathbb{F}_v^{\text{sep}}/\mathbb{F}_v, \tilde{E})_p.$$

We can now conclude by a theorem of Lang from which we deduce the triviality of $H^1(\mathbb{F}_v^{\text{sep}}/\mathbb{F}_v, \tilde{E})$:

Theorem 2.15 (Lang). Let A be a smooth, connected, commutative algebraic group over a finite field k . Then $H^1(k, A(\bar{k})) = 0$.

Case 2. $v \nmid n$ but $v|N$.

Consider a Néron model \mathcal{E} for E over \mathcal{O}_v and let \mathcal{E}_0 be the connected component of the identity of \mathcal{E} and $\mathcal{E}^0/\mathcal{E}$ the group of components.

As a consequence of Lang's theorem (2.15) we have that $H^1(\mathbb{F}_v^{\text{sep}}/\mathbb{F}_v, \mathcal{E}^0) = 0$. So we have an injection

$$H^1(K_v^{\text{ur}}/K_v, \mathcal{E}^0) \hookrightarrow H^1(\mathbb{F}_v^{\text{sep}}/\mathbb{F}_v, \mathcal{E}/\mathcal{E}^0).$$

Hence to check the triviality of $d(n)_v$ we need to check it in the cohomology group $H^1(\mathbb{F}_v^{\text{sep}}/\mathbb{F}_v, \mathcal{E}/\mathcal{E}^0)$.

Let w be a place of K_n above v . We recall that $d(n)_v$ is represented by the cocycle:

$$\begin{array}{ccc} \text{Gal}((K_n)_w/K_v) & \longrightarrow & E((K_n)_w) \\ \gamma & \longmapsto & -\frac{(\gamma-1)P_n}{p}, \end{array}$$

where $-\frac{(\gamma-1)P_n}{p}$ is a combination of the elements $y_n \in E(K_n)$. To prove the triviality of $d(n)_v$, which is killed by p , we are going to prove that the image of the reduction of y_n in $\mathcal{E}/\mathcal{E}^0$ lies in a subgroup of order prime to p .

From ([GZ86]; III, 3.1) we deduce that the class of the Heegner divisor $(x_n) - (\infty)$ lies, up to translation by the rational torsion point $(0) - (\infty)$, in $J(X_0(N))$, in $J(X_0(N))^{01}$

¹ $J(X_0(N))^{01}$ is the identity component of the Néron model of the abelian variety $J(X_0(N))$ over \mathcal{O}_v .

Hence y_n is, up to translation by the rational torsion of \mathcal{E} , in \mathcal{E}^0 . Since $E(\mathbb{Q})_p = 0$ by assumption the points y_n lie in a subgroup whose image in $\mathcal{E}/\mathcal{E}^0$ has order prime to p , so we are done. \square

Proposition 2.16. If $n = lm$ and λ is the unique prime of K dividing l , the class $d(n)_\lambda$ is locally trivial in $H^1(K_\lambda, E)_p$ if and only if $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$ for one (and hence all) places λ_m of K_m dividing λ .

Proof. We recall that the prime λ splits completely in K_m , each factor λ_m is totally ramified in K_n , i.e. $\lambda_m \mathcal{O}_{K_n} = (\lambda_n)^{l+1}$, and $\mathbb{F}_{\lambda_n} = \mathbb{F}_{\lambda_m} = \mathbb{F}_\lambda$. By construction the localisation of $d(n)_\lambda \in H^1(K_\lambda, E)_p$ actually lives in $H^1(G_l, E(K_{\lambda_n}))_p$, since $d(n)$ goes to zero in $H^1(K_n, E)_p^{G_n}$, and it is represented by the cocycle:

$$\begin{aligned} G_l &\longrightarrow E(K_{\lambda_n}) \\ \sigma &\longmapsto -\frac{(\sigma-1)P_n}{p}. \end{aligned}$$

Since l does not divide N by assumption, E has good reduction at l . So we can construct a minimal Weierstrass model \mathcal{E} for E over K_λ , which is also a Néron model by example (0.12), defined over \mathbb{Z}_l and such that $\mathcal{E}(\mathcal{O}_{\lambda_n}) \simeq E(K_{\lambda_n})$.

We know that there exists an exact sequence of G_l -modules, sequence (0.7):

$$0 \rightarrow E_1(K_{\lambda_n}) \rightarrow E_0(K_{\lambda_n}) \xrightarrow{\text{red}} \tilde{E}(\mathbb{F}_{\lambda_n}) \rightarrow 0$$

As we have already remarked in the proof of proposition (2.14) $H^1(G_l, E_1(K_{\lambda_n}))_p = 0$.

So we have an injection:

$$H^1(G_l, E(K_{\lambda_n}))_p \hookrightarrow H^1(G_l, \tilde{E}(\mathbb{F}_\lambda))_p$$

where $H^1(G_l, \tilde{E}(\mathbb{F}_\lambda))_p = \text{Hom}(G_l, \tilde{E}(\mathbb{F}_\lambda)_p)$, since G_l acts trivially on $\tilde{E}(\mathbb{F}_\lambda)$. Hence $d(n)_\lambda$ is trivial if and only if it has trivial image in $H^1(G_l, \tilde{E}(\mathbb{F}_\lambda))_p$, so if and only if $-\frac{(\sigma-1)P_n}{p}$ has trivial reduction modulo λ_n for every $\sigma \in G_l$, or equivalently if and only if the point

$$Q_n := \frac{(\sigma_l - 1)P_n}{p}$$

has trivial reduction modulo λ_n , for σ_l the generator of G_l .

Recall that $P_n = \sum_S \sigma D_m \cdot D_l \cdot y_n$ and $(\sigma_l - 1)D_l = l + 1 - \text{Tr}_l$ so

$$Q_n = \sum_S \sigma D_m \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right)$$

by proposition (2.7) we have the congruence:

$$\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \equiv \frac{(l+1)\text{Frob}(\lambda_m) - a_l}{p} y_m \pmod{\lambda_n}$$

at all primes λ_n dividing λ in K_n . For $\sigma \in \text{Gal}(K_n/K)$ we conjugate this congruence modulo by σ to obtain:

$$\sigma \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \sigma \left(\frac{(l+1)\text{Frob}(\sigma^{-1}\lambda_m) - a_l}{p} \right) y_m \pmod{\lambda_n},$$

but $\sigma\text{Frob}(\sigma^{-1}\lambda_m) = \sigma\sigma^{-1}\text{Frob}(\lambda_m)\sigma$ so we obtain:

$$\sigma \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \left(\frac{(l+1)\text{Frob}(\lambda_m) - a_l}{p} \right) \sigma y_m \pmod{\lambda_n}$$

Hence:

$$Q_n \equiv \frac{(l+1)\text{Frob}(\lambda_m) - a_l}{p} P_m \pmod{\lambda_n}$$

We know by proposition (2.13) that the reduction of P_m modulo λ_m lies in the ϵ_m -eigenspace of $\tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda)$ for the action of complex conjugation τ .

Consider the eigenspaces $\tilde{E}(\mathbb{F}_\lambda)^+, \tilde{E}(\mathbb{F}_\lambda)^- \subset \tilde{E}(\mathbb{F}_\lambda)$.

On the eigenspace $\tilde{E}(\mathbb{F}_\lambda)^+$ the automorphism $\text{Frob}(\lambda_m)$ acts as the identity, since we made the assumption that l is a 'Kolyvagin's prime', so that $\tau \in \text{Frob}(\lambda_m)$. Hence $(l+1)\text{Frob}(\lambda_m) - a_l$ acts as multiplication by $l+1-a_l$, which is the order of $\tilde{E}(\mathbb{F}_\lambda)^+$, by the proof of proposition (2.6). Moreover on the eigenspace $\tilde{E}(\mathbb{F}_\lambda)^-$ the automorphism $\text{Frob}(\lambda_m)$ acts as minus the identity so that $(l+1)\text{Frob}(\lambda_m) - a_l$ acts as the multiplication by minus the order of $\tilde{E}(\mathbb{F}_\lambda)^-$, also by (2.6). In any case we conclude that $(l+1)\text{Frob}(\lambda_m) - a_l$ kills $\tilde{E}(\mathbb{F}_\lambda)$.

The reduction of P_m modulo λ_n lies in $\tilde{E}(\mathbb{F}_\lambda)_p^{\epsilon_m} \simeq \mathbb{Z}/p\mathbb{Z}$, by proposition (2.13). So the reduction \tilde{Q}_n of Q_n is zero if and only if $\tilde{P}_m/p \in \tilde{E}(\mathbb{F}_\lambda)_p$, i.e. $\tilde{P}_m \in p\tilde{E}(\mathbb{F}_\lambda)$, which is if and only if $P_m \in p(K_\lambda)$, since p is an isomorphism on E_1 . \square

2.6 Tate local duality.

In this section we are going to review some basic results from Tate's local duality which we will use in order to prove Proposition (2.3).

Let \mathcal{O}_λ be a complete discrete valuation ring with finite residue field $\mathbb{F}_\lambda = \mathcal{O}_\lambda/\mathfrak{m}$ of characteristic l and field of fractions K_λ .

Let K_λ^{ur} be the maximal unramified extension of K_λ , with Galois group

$$\mathfrak{g} = \text{Gal}(K_\lambda^{\text{ur}}/K_\lambda) \simeq \text{Gal}(\mathbb{F}_\lambda^{\text{sep}}/\mathbb{F}_\lambda),$$

which is isomorphic to $\hat{\mathbb{Z}}$ by sending the generator $1 \in \hat{\mathbb{Z}}$ to the Frobenius automorphism $\text{Frob}(\lambda) \in \mathfrak{g}$.

Let E be an elliptic curve over K_λ , with good reduction over \mathcal{O}_λ .

Let p be a prime different from l , since E has good reduction over \mathcal{O}_l , we have the following exact sequence for the reduced elliptic curve \tilde{E} over \mathbb{F}_λ :

$$0 \rightarrow \tilde{E}_p \rightarrow \tilde{E} \xrightarrow{p} \tilde{E} \rightarrow 0,$$

which induces the exact sequence in cohomology:

$$0 \rightarrow \tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda) \rightarrow H^1(\mathfrak{g}, \tilde{E}(\mathbb{F}_\lambda^{\text{sep}}))_p \rightarrow H^1(\mathfrak{g}, \tilde{E}(\mathbb{F}_\lambda^{\text{sep}})_p) \rightarrow 0,$$

where the last group is zero by Lang's theorem (2.15).

So we obtain:

$$\tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda) \xrightarrow{\sim} H^1(\mathfrak{g}, \tilde{E}(\mathbb{F}_\lambda^{\text{sep}})_p)$$

Moreover from (0.8) and (0.9) we have isomorphisms:

$$E(K_\lambda)/pE(K_\lambda) \simeq \tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda) \text{ and } E_p := E(\overline{K_\lambda})_p = \tilde{E}(\mathbb{F}_\lambda^{\text{sep}})_p = E(K_\lambda^{\text{un}}).$$

So we obtain:

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} H^1(\mathfrak{g}, E_p). \quad (2.9)$$

Now we recall Tate's local duality theorem.

Theorem 2.17 (Tate-local duality). There exists a symmetric, non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$ -vector spaces:

$$\langle \cdot, \cdot \rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \rightarrow \mathbb{Z}/p\mathbb{Z} \quad (2.10)$$

induced by Weil pairing, cup product and the invariant map from local class field theory.

Proof. (sketch of the construction) The Weil pairing $E_p \times E_p \rightarrow \mu_p$ over K_λ induces a linear map

$$E_p \otimes E_p \rightarrow \mu_p$$

, which induces a map on cohomology groups for every $j \geq 0$:

$$H^j(K_\lambda, E_p \otimes E_p) \rightarrow H^j(K_\lambda, \mu_p),$$

since Weil pairing is Galois equivariant.

So composing cup product with this map for $j = 2$ we obtain a pairing:

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \rightarrow H^2(K_\lambda, \mu_p).$$

Moreover the invariant map from local class field theory gives a canonical isomorphism:

$$H^2(K_\lambda, \mu_p) = \text{Br}(K_\lambda)_p \xrightarrow{\sim} \frac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}.$$

□

Proposition 2.18. The group $H^1(\mathfrak{g}, E_p)$ is isotropic for the pairing $\langle \cdot, \cdot \rangle$ of (2.10).

Proof. Being isotropic means that if we compute the pairing on elements of $H^1(\mathfrak{g}, E_p) \times H^1(\mathfrak{g}, E_p)$ we get zero. Consider the following diagram:

$$\begin{array}{ccc}
H^1(\mathfrak{g}, E_p) \times H^1(\mathfrak{g}, E_p) & \xrightarrow{\text{Inf} \times \text{Inf}} & H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \\
\downarrow & & \downarrow \\
H^2(\mathfrak{g}, \mu_p) & \xrightarrow{\text{Inf}} & H^2(K_\lambda, \mu_p) \\
\parallel & & \downarrow \\
0 & & \mathbb{Z}/p\mathbb{Z}
\end{array}$$

where $H^2(\mathfrak{g}, \mu_p) = 0$ from Lang's theorem (2.15). \square

Now consider the following commutative diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & E(K_\lambda)/pE(K_\lambda) & \longrightarrow & H^1(K_\lambda, E_p) & \longrightarrow & H^1(K_\lambda, E)_p \longrightarrow 0 \\
& & \downarrow & & \sim \downarrow & & \downarrow \\
0 & \longrightarrow & H^1(K_\lambda, E)_p^* & \longrightarrow & H^1(K_\lambda, E_p)^* & \longrightarrow & (E(K_\lambda)/pE(K_\lambda))^* \longrightarrow 0
\end{array}$$

where $\cdot^* = \text{Hom}_{\mathbb{Z}}(\cdot, \mu(\overline{K}_\lambda))$ is the Cartier Dual, rows are exact and the middle map is an isomorphism by Tate local duality.

Since $E(K_\lambda)/pE(K_\lambda) \simeq H^1(\mathfrak{g}, E_p)$ is isotropic for the pairing we know that the first vertical map is injective, but in fact it also an isomorphism since we have the following:

Lemma 2.19. $\dim_{\mathbb{Z}/p\mathbb{Z}} E(K_\lambda)/pE(K_\lambda) = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(K_\lambda, E)_p$.

Proof. Since we have the exact sequence:

$$0 \rightarrow \ker(\text{Frob}(\lambda) - 1) \rightarrow E_p \rightarrow E_p \rightarrow E_p/(\text{Frob}(\lambda) - 1)E_p \rightarrow 0,$$

then we know that $E_p^{\{\text{Frob}(\lambda)=1\}}$ and $E_p/(\text{Frob}(\lambda) - 1)E_p$ have the same dimension over \mathbb{F}_p .

So since we have:

$$E(K_\lambda)/pE(K_\lambda) \simeq H^1(\mathfrak{g}, E_p) = E_p/(\text{Frob}(\lambda) - 1)E_p$$

and

$$E_p^{\{\text{Frob}(\lambda)=1\}} = \widetilde{E}(\mathbb{F}_\lambda)_p \simeq E(K_\lambda)_p,$$

we can deduce that $E(K_\lambda)/pE(K_\lambda)$ and $E(K_\lambda)_p$ have the same dimension over \mathbb{F}_p .

So we can check the following equality of dimensions:

$$\dim_{\mathbb{Z}/p\mathbb{Z}} E(K_\lambda)_p = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(K_\lambda, E)_p.$$

Consider the first terms of the Hochschild-Serre spectral sequence for the group $\mathfrak{g} \leq \text{Gal}(\overline{K}_\lambda/K_\lambda)$:

$$0 \rightarrow H^1(\mathfrak{g}, E(K_\lambda^{\text{ur}})_p) \rightarrow H^1(K_\lambda, E_p) \rightarrow H^1(K_\lambda^{\text{ur}}, E_p)^{\text{Frob}(\lambda)} \rightarrow H^2(\mathfrak{g}, E(K_\lambda^{\text{ur}})_p),$$

where the last group is zero from a result in Galois cohomology which uses the fact that E_p is torsion.

We also have:

$$0 \rightarrow E(K_\lambda)/pE(K_\lambda) \rightarrow H^1(K_\lambda, E_p) \rightarrow H^1(K_\lambda, E)_p \rightarrow 0.$$

So since $H^1(\mathfrak{g}, E_p) \simeq E(K_\lambda)/E(K_\lambda)$ then there exists an isomorphism:

$$H^1(K_\lambda, E)_p \xrightarrow{\sim} H^1(K_\lambda^{\text{ur}}, E_p)^{\text{Frob}(\lambda)},$$

but the inertia group $\mathcal{I} = \text{Gal}(\overline{K}_\lambda/K_\lambda^{\text{ur}})$ sits in the exact sequence

$$1 \rightarrow \mathcal{P} \rightarrow \mathcal{I} \rightarrow \Delta \rightarrow 1,$$

where \mathcal{P} is the wildly ramified inertia subgroup and Δ is the tamely ramified inertia subgroup.

\mathcal{P} is a pro- l group so its cohomology vanishes for degrees bigger than 0, which means that

$$H^1(K_\lambda^{\text{ur}}, E_p) = H^1(\mathcal{I}, E_p) \simeq H^1(\Delta, E_p),$$

with Δ acting trivially on $E_p = E(K_\lambda^{\text{ur}})_p$.

Moreover we know that $\Delta \simeq \prod_{q \neq l} \mathbb{Z}_q(1)$, as a \mathfrak{g} -module, where $\mathbb{Z}_q(1)$ is the Tate module of the q -roots of unity, so we have:

$$\text{Hom}(\Delta, E_p)^{\text{Frob}(\lambda)} \simeq \text{Hom}(\mathbb{Z}_p(1), E_p)^{\text{Frob}(\lambda)} \simeq \text{Hom}(\mu_p, E_p)^{\text{Frob}(\lambda)},$$

where the last group has the same dimension of $\tilde{E}(\mathbb{F}_\lambda)_p \simeq E(K_\lambda)_p$ by Weil pairing.

To summarize:

$$\dim_{\mathbb{Z}/p\mathbb{Z}} H^1(K_\lambda, E)_p = \dots = \dim_{\mathbb{Z}/p\mathbb{Z}} \tilde{E}(\mathbb{F}_\lambda)_p = \dim_{\mathbb{Z}/p\mathbb{Z}} E(K_\lambda)_p,$$

which is what we wanted to prove. \square

So we can now conclude that

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} H^1(K_\lambda, E)_p^*$$

and we have :

Proposition 2.20. The pairing $\langle \cdot, \cdot \rangle$ of (2.10) induces a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$ -vector spaces

$$\langle \cdot, \cdot \rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \longrightarrow \mathbb{Z}/p\mathbb{Z}. \quad (2.11)$$

Moreover we would like to remark that in the case when the p -torsion of E is rational over K_λ there exists an explicit formula for the pairing $\langle \cdot, \cdot \rangle$ of (2.11).

Indeed, take $c_1 \in E(K_\lambda)/pE(K_\lambda)$ and construct the point $e_1 = \left(\frac{1}{p}c_1\right)^{\text{Frob}(\lambda)-1}$ in $E(K_\lambda)_p$ then take $c_2 \in H^1(K_\lambda, E_p)$ and associate to it the homomorphism $\phi_2 : \mu_p \rightarrow E(K_\lambda)_p$ as in the proof of (2.19). Fix a primitive p^{th} -root ξ of unity in K_λ^\times and let $\phi_2(\xi) = e_2$ in $E(K_\lambda)_p$. Then:

$$\xi^{\langle c_1, c_2 \rangle} = \{e_1, e_2\},$$

where $\{, \}$ is the Weil pairing on E_p .

A proof of this construction may be found in an appendix of [Was89].

2.7 Computation of the Selmer group.

In this section we are going to apply the results of the last section in our situation in order to bound the order of the p -Selmer group of the elliptic curve and prove proposition (2.3).

Consider the completion of the imaginary quadratic field K at the inert prime λ which lies above l .

First of all we claim that the p -torsion of E is rational over K_λ .

In fact we assumed in (2.3) that l was a Kolyvagin prime, which implies that λ splits completely in $K(E_p)$. From this we deduce that if γ is a prime of $K(E_p)$ above λ , then $\mathbb{F}_\gamma \simeq \mathbb{F}_\lambda$, so that

$$\tilde{E}(\mathbb{F}_\lambda)_p \simeq \tilde{E}(\mathbb{F}_\gamma)_p \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Moreover from (0.9) we have $E(K_\lambda)_p \simeq \tilde{E}(\mathbb{F}_\lambda)$ and so the claim.

In this situation the spaces involved in the pairing (2.11) have each dimension 2 over $\mathbb{Z}/p\mathbb{Z}$. However we wish to work with spaces of dimension 1, so we shall consider the action of complex conjugation on these spaces.

Recall that from proposition (2.6) we had $E_p(K_\lambda)^\pm = \tilde{E}(\mathbb{F}_\lambda)_p^\pm \simeq \mathbb{Z}/p\mathbb{Z}$.

We shall show that there exists a similar decomposition for the spaces $E(K_\lambda)/pE(K_\lambda)$ and $H^1(K_\lambda, E)_p$.

Lemma 2.21. The eigenspaces $(E(K_\lambda)/pE(K_\lambda))^\pm$ and $H^1(K_\lambda, E)_p^\pm$ for $\text{Gal}(K_\lambda/\mathbb{Q}_l) = \text{Gal}(K/\mathbb{Q}) = \{1, \tau\}$ each have dimension 1 over $\mathbb{Z}/p\mathbb{Z}$.

Proof. We have isomorphisms of $\text{Gal}(K_\lambda/\mathbb{Q}_l)$ -modules:

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} E(K_\lambda)_p \text{ and } H^1(K_\lambda, E)_p \xrightarrow{\sim} \text{Hom}(\mu_p, E_p).$$

From the congruence $l + 1 \equiv 0 \pmod{p}$ we deduce that

$$\mu_p(\overline{K_\lambda}) = \mu_p(K_\lambda),$$

in fact from Hensel's lemma we can look for the p -roots of unity defined over K_λ in \mathbb{F}_λ , which contains them all since p divides $l^2 - 1$, the order of $\mathbb{F}_\lambda^\times$. Moreover, since p does not divide $l - 1$, p is odd, $\mu_p(\mathbb{Q}_l) = \{1\}$, which implies

$$\mu_p(K_\lambda) = \mu_p(K_\lambda)^-.$$

So we have $\text{Hom}(\mu_p, E_p) \simeq E(K_\lambda)_p$ as groups, but with reversed action, i.e.

$$H^1(K_\lambda, E)_p^\pm \simeq \text{Hom}(\mu_p, E_p)^\pm \simeq E(K_\lambda)_p^\mp.$$

□

Proposition 2.22. The pairing $\langle \cdot, \cdot \rangle$ of (2.11) induces non-degenerate pairings of one dimensional $\mathbb{Z}/p\mathbb{Z}$ -vector spaces

$$\langle \cdot, \cdot \rangle^\pm : (E(K_\lambda)/pE(K_\lambda))^\pm \times H^1(K_\lambda, E)_p^\pm \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

In particular if $d_\lambda \neq 0$ lies in $H^1(K_\lambda, E)_p^\pm$ and $s_\lambda \in (E(K_\lambda)/pE(K_\lambda))^\pm$ satisfies $\langle s_\lambda, d_\lambda \rangle = 0$, then $s_\lambda \equiv 0 \pmod{pE(K_\lambda)}$.

Proof. It suffices to check that the $+$ and $-$ eigenspaces for complex conjugation are orthogonal under $\langle \cdot, \cdot \rangle$.

Tate's pairing satisfies $\langle c_1^\tau, c_2^\tau \rangle = \langle c_1, c_2 \rangle^\tau = \langle c_1, c_2 \rangle$, since τ acts trivially on $H^2(K_\lambda, \mu_p) \simeq \mathbb{Z}/p\mathbb{Z}$, so the result follows. □

Now we shall apply the preceding considerations to classes which belong to the p -Selmer group of the elliptic curve E , but for the proof we need to recall a result from global class field theory.

Theorem 2.23. Given a number field K , recall that for a field L the Brauer group is defined as $\text{Br}(L) = H^2(L, \overline{L}^\times)$. There exists the following short exact sequence:

$$0 \rightarrow \text{Br}(K) \longrightarrow \bigoplus_v \text{Br}(K_v) \longrightarrow \frac{\mathbb{Q}}{\mathbb{Z}} \rightarrow 0,$$

where the first map is a product of restriction maps and the second one is the summation over the local invariants $\text{inv}_v : \text{Br}(K_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ and possibly $\text{inv}_\infty : \text{Br}(\mathbb{R}) \xrightarrow{\sim} 1/2\mathbb{Z}/\mathbb{Z}$.

Proposition 2.24. Assume that a class $d \in H^1(K, E)_p^\pm$ is locally trivial at all places $v \neq \lambda$, but that $d_\lambda \neq 0$ in $H^1(K_\lambda, E)_p^\pm$. Then for any class $s \in \text{Sel}(E/K)_p^\pm \subset H^1(K, E_p)^\pm$ we have $s_\lambda = 0$ in $H^1(K_\lambda, E_p)^\pm$.

Proof. The restriction $s_\lambda \in H^1(K_\lambda, E_p)^\pm$ of s lies in $(E(K_\lambda)/pE(K_\lambda))^\pm$, by definition of the p -Selmer group. So by proposition (2.22) we only need to check that $\langle s_\lambda, d_\lambda \rangle = 0$ to conclude the proof.

To do this, lift $d \in H^1(K, E)_p$ to an element $c \in H^1(K, E_p)$, which is well defined modulo $E(K)/pE(K)$. Consider the global pairing $\langle s, c \rangle_K$ induced by cup product and Weil pairing, which is construction in the same way as in (2.10), but in this case K is a number field and not a local field. The image $\langle s, c \rangle_K$ lies in $H^2(K, \mu_p) = \text{Br}(K)_p$. So from theorem (2.23) we deduce that if we push $\langle s, c \rangle_K$ to \mathbb{Q}/\mathbb{Z} we obtain zero, i.e.

$$\sum_v \text{inv}_v(\langle s_v, c_v \rangle) = 0,$$

but we already know from the hypothesis that $\langle s_v, c_v \rangle = 0$ for every $v \neq \lambda$, since $d_v = 0$ in $H^1(K_v, E_p)$. So this implies that

$$\sum_v \text{inv}_v(\langle s_v, c_v \rangle) = \langle s_\lambda, c_\lambda \rangle = \langle s_\lambda, d_\lambda \rangle = 0.$$

□

Now we wish to use the cohomology classes $d = d(n) \in H^1(K, E)_p$, constructed in section (2.4), to bound the order of $\text{Sel}_p(E/K)$, but before we need a few more Galois cohomology computations.

Call $L := K(E_p)$ and recall that we have assumed:

$$\mathcal{G} := \text{Gal}(L/K) = \text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Proposition 2.25. $H^n(\mathcal{G}, E_p) = 0$ for all $n \geq 0$ and restriction induces an isomorphism:

$$\text{Res}: H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^\mathcal{G} = \text{Hom}_\mathcal{G}(\text{Gal}(\overline{\mathbb{Q}}/L), E_p)$$

Proof. $\mathcal{G} \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has a central subgroup Z isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ which acts as homotheties on the torsion points E_p .

Since p is odd $Z \neq \{1\}$, so that $E_p^Z = H^0(Z, E_p) = 0$, moreover since Z has order $p-1$, which is prime to p , we also have $H^i(Z, E_p) = 0$ for all $i > 0$.

We can now consider the Hochschild-Serre spectral sequence:

$$H^m(\mathcal{G}/Z, H^n(Z, E_p)) \Rightarrow H^{m+n}(\mathcal{G}, E_p)$$

to conclude that $H^n(\mathcal{G}, E_p) = 0$ for all $n \geq 0$.

On the other hand we have another spectral sequence induced by $\mathcal{G} \leq \text{Gal}(\overline{K}/K)$:

$$0 \rightarrow H^1(\mathcal{G}, E_p) \xrightarrow{\text{Inf}} H^1(K, E_p) \xrightarrow{\text{Res}} H^1(L, E_p)^{\mathcal{G}} \rightarrow H^2(\mathcal{G}, E_p).$$

The vanishing of $H^n(\mathcal{G}, E_p)$ for $n = 1, 2$ gives us the isomorphism in the proposition. \square

From the last proposition we deduce that there exists a pairing:

$$[\cdot, \cdot] : H^1(K, E_p) \times \text{Gal}(\overline{\mathbb{Q}}/L) \rightarrow E_p$$

which satisfies for all $\sigma \in \mathcal{G}$: $[s, \sigma(\rho)] = \sigma([s, \rho])$ for all $s \in H^1(K, E_p)$, $\rho \in \text{Gal}(\overline{\mathbb{Q}}/L)$ and is such that if $[s, \rho] = 0$ for all $\rho \in \text{Gal}(\overline{\mathbb{Q}}/K)$ then $s = 0$.

Now let $S \subset H^1(K, E_p)$ be a finite subgroup, we shall eventually apply this reasoning to $S = \text{Sel}_p(E/K)$. Let

$$\text{Gal}_S(\overline{\mathbb{Q}}/L) := \{\rho \in \text{Gal}(\overline{\mathbb{Q}}/L) \mid [s, \rho] = 0 \text{ for all } s \in S\} \quad (2.12)$$

and let L^S be the fixed field of $\text{Gal}_S(\overline{\mathbb{Q}}/L)$.

Then L^S is a finite normal extension of L .

Lemma 2.26. There is an induced pairing

$$[\cdot, \cdot] : S \times \text{Gal}(L^S/L) \rightarrow E_p,$$

which is non-degenerate and which induces an isomorphism of $\mathcal{G} = \text{Gal}(L/K)$ -modules:

$$\text{Gal}(L^S/L) \xrightarrow{\sim} \text{Hom}(S, E_p),$$

as well as an isomorphism of $\text{Gal}(K/\mathbb{Q})$ -modules:

$$S \xrightarrow{\sim} \text{Hom}_{\mathcal{G}}(\text{Gal}(L^S/L), E_p).$$

Proof. We have the following injections, which follow from the definition of L^S and proposition (2.25),:

$$\text{Gal}(L^S/L) \hookrightarrow \text{Hom}(S, E_p). \quad (2.13)$$

and

$$S \hookrightarrow \text{Hom}_{\mathcal{G}}(\text{Gal}(L^S/L), E_p). \quad (2.14)$$

We wish to show that they are actually isomorphisms, let us compute dimensions.

If $r = \dim_{\mathbb{Z}/p\mathbb{Z}}(S)$, from (2.13) we deduce that $\text{Gal}(L^S/L)$ is a \mathcal{G} -submodule of $\text{Hom}(S, E_p) \simeq E_p^r$. E_p is a simple \mathcal{G} -module, then E_p^r is semi-simple. Any

submodule of a semi-simple module is semi-simple, so we have an isomorphism:

$$\mathrm{Gal}(L^S/L) \xrightarrow{\sim} E_p^s \text{ for some } s \leq r.$$

Hence:

$$\mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L^S/L), E_p) \simeq (\mathbb{Z}/p\mathbb{Z})^s$$

since $\mathrm{Hom}_{\mathcal{G}}(E_p, E_p) \simeq \mathbb{Z}/p\mathbb{Z}$, in fact \mathcal{G} is the full group of automorphisms of $L = K(E_p)$ and so the only automorphisms which commute with all of the others are the scalars.

This group contains $S \simeq (\mathbb{Z}/p\mathbb{Z})^r$ by (2.14), so we must have $s \geq r$ which implies $s = r$ and the proof. \square

We would now like to apply lemma (2.26) to $S = \mathrm{Sel}_p(E/K)$.

For simplicity of notation let $M = L^S$ and $H = \mathrm{Gal}(M/L) = \mathrm{Gal}(L^S/L)$.

Since we eventually want to get to the proof of proposition (2.3), let $y_K \in E(K)$, as in (1.11), have infinite order and let it not be divisible by p in $E(K)/E(K)_{\mathrm{tors}}$, $\delta y_K \in \mathrm{Sel}_p(E/K)$ is its non-zero image inside the p -Selmer group.

Let I be the subgroup of H which fixes the subfield $L(\frac{1}{p}y_K)$.

We have the following field diagram:

$$\begin{array}{ccc}
 & M & \\
 & | & \searrow I \\
 H \simeq \mathrm{Hom}(\mathrm{Sel}_p(E/K), E_p) & & L(\frac{1}{p}y_K) \\
 & | & \nearrow E_p \\
 L = K(E_p) & & \\
 & | \mathcal{G} \simeq \mathrm{Aut}(E_p) & \\
 & K & \\
 & | & \\
 & \mathbb{Q} &
 \end{array}$$

Let τ be a fixed lifting of complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$ and let H^+ and I^+ denote the +1 eigenspaces for τ in H and I .

Lemma 2.27. $H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in I\}$ and $H^+/I^+ \simeq \mathbb{Z}/p\mathbb{Z}$.

Proof. We have $H^+ = H^{\tau+1}$. Indeed clearly $H^{\tau+1} \subset H^+$, since $(H^{\tau+1})^{\tau-1} = H^{\tau^2-1} = \mathrm{id}$ implies $H^{\tau+1} \subset H^+$, and, since p is odd and H is a $\mathbb{Z}/p\mathbb{Z}$ -vector space, 2 is an automorphism of H which implies that if $h \in H^+$ then $h = (h^{1/2})^{\tau+1}$ so that $h \in H^{\tau+1}$. Then we have

$$H^+ = H^{\tau+1} = \{(\tau h)^2 : h \in H\},$$

since $\tau^{-1} = \tau$. The same reasoning works for I^+ . Finally $H^+/I^+ = (H/I)^+ = E_p^+ \simeq \mathbb{Z}/p\mathbb{Z}$. \square

Proposition 2.28. Let $s \in \text{Sel}_p(E/K)^\pm$.

Then the following are equivalent:

- a. $[s, \rho] = 0$ for all $\rho \in H$,
- b. $[s, \rho] = 0$ for all $\rho \in H^+$,
- c. $[s, \rho] = 0$ for all $\rho \in H^+ \setminus I^+$,
- d. $s = 0$.

Proof. d. \Leftrightarrow a. from lemma (2.26) and clearly a. \Rightarrow b. \Rightarrow c.

So it suffices to prove c. \Rightarrow a.

Since $s : H^+ \rightarrow E_p$ is a group homomorphism and $I^+ \neq H^+$, the fact that s vanishes on $H^+ \setminus I^+$ implies that it vanishes on the entire group H^+ . Let us suppose that $s \in \text{Sel}_p(E/K)^+$, then s induces a \mathcal{G} -homomorphism $H \rightarrow E_p$, see (2.14), which maps $H^+ \rightarrow E_p^+$ and $H^- \rightarrow E_p^-$. If s vanishes on H^+ , the image $s(H)$ is therefore contained in E_p^- , but $s(H)$ is a \mathcal{G} -submodule of the simple \mathcal{G} -module E_p , so if $s(H) \neq E_p$ we must have $s(H) = 0$, which implies a. The same reasoning is valid for $s \in \text{Sel}_p(E/K)^-$ with $+$ and $-$ reversed. \square

Now let λ be a prime of K which does not divide $N \cdot p$. Then λ is unramified in M/K ; we assume further that λ splits completely in L/K and let λ_M be a prime of M above λ . Let Fr_{λ_M} be the Frobenius substitution of the prime λ_M in $\text{Gal}(M/K)$, then $\text{Fr}_{\lambda_M} \in H \simeq \text{Hom}(\text{Sel}_p(E/K), E_p)$ and the \mathcal{G} -orbit of λ_M depends only on λ , call it $\text{Frob}(\lambda)$. By definition we will write $[s, \text{Frob}(\lambda)] = 0$ if and only if $[s, \rho] = 0$ for every $\rho \in \text{Frob}(\lambda)$.

Proposition 2.29. For $s \in \text{Sel}_p(E/K) \subset H^1(K, E_p)$ the following are equivalent:

- a. $[s, \text{Fr}_{\lambda_M/\lambda}] = 0$.
- b. $[s, \text{Frob}(\lambda)] = 0$.
- c. $s_\lambda = 0$ in $H^1(K_\lambda, E_p)$.

Proof. The pairing of lemma (2.26) satisfies:

$$[s, \sigma(\rho)] = \sigma([s, \rho]) \text{ for all } \sigma \in \mathcal{G},$$

so clearly a. is equivalent to b., since by definition $\text{Frob}(\lambda)$ is the \mathcal{G} -orbit of $\text{Fr}_{\lambda_M/\lambda}$.

Now consider the element $P_\lambda \in E(K_\lambda)/pE(K_\lambda)$ which image in $H^1(K_\lambda, E_p)$, through the injection $E(K_\lambda)/pE(K_\lambda) \hookrightarrow H^1(K_\lambda, E_p)$, is $s_\lambda \in \text{Sel}_p(E/K)$, then, by definition, $\frac{1}{p}P_\lambda \in E(M_{\lambda_M})$. We have:

$$[s, \text{Fr}_{\lambda_M/\lambda}] = \text{Fr}_{\lambda_M/\lambda}\left(\frac{1}{p}P_\lambda\right) - \frac{1}{p}P_\lambda \text{ in } E(M_{\lambda_M}) = E(M)_p$$

Hence $[s, \text{Fr}_{\lambda_M/\lambda}] = 0$ if and only if $\frac{1}{p}P_\lambda \in E(K_\lambda)$ if and only if $P_\lambda \in pE(K_\lambda)$ if and only if condition c. holds. \square

We now finally turn to the proof of proposition (2.3). Recall that the Heegner point $y_K = P_1$ lies in the ϵ -eigenspace for complex conjugation on $E(K)/pE(K)$, where ϵ is the eigenvalue of the Fricke involution on the newform f associated to E . Hence $\delta y_K \in \text{Sel}_p(E/K)^\epsilon$.

Lemma 2.30. $\text{Sel}_p(E/K)^{-\epsilon} = 0$.

Proof. Assume that $s \in \text{Sel}_p(E/K)^{-\epsilon}$. To show that $s = 0$ it suffices, by proposition (2.28), to show that $[s, \rho] = 0$ for every $\rho \in H^+ \setminus I^+$. An element of H^+ is of the form $(\tau h)^2$, for some $h \in H$, by proposition (2.27).

Let l be a prime which is unramified in the extension M/\mathbb{Q} and such that there is a factor λ_M above it in M , whose Frobenius substitution equals τh in $\text{Gal}(M/\mathbb{Q})$. The density of such primes is positive by Chebotarev density theorem and so we can always find a prime satisfying that condition. Then $(l) = \lambda$ is inert in K and λ splits completely in L . The Frobenius substitution of $\mathbb{F}_{\lambda_M}/\mathbb{F}_\lambda$ is equal to $(\tau h)^2$, so to prove that $[s, \rho] = [s, (\tau h)^2] = 0$ it suffices, by proposition (2.29), to show that $s_\lambda \equiv 0$ in $H^1(K_\lambda, E_p)$. Let $c(l) \in H^1(K, E_p)$ and $d(l) \in H^1(K, E)_p$ be the cohomology classes constructed in section (2.4). By proposition (2.13) both classes lie in the $-\epsilon$ -eigenspace for complex conjugation and, by proposition (2.14), $d(l)$ is locally trivial except at λ . We claim that $d(l)_\lambda \neq 0$ in $H^1(K, E)_p$. Indeed, by proposition (2.16), $d(l)_\lambda = 0$ if and only if $y_K = P_1 \in pE(K_\lambda)$, or equivalently if and only if the prime λ splits completely in the extension $L(\frac{1}{p}y_K)$. Since $\text{Fr}_{\lambda_M/\lambda} = \rho$ is not in $I^+ = I \cap H^+$ by hypothesis, this splitting does not occur. So we can apply proposition (2.28) to deduce that $s \in \text{Sel}_p(E/K)^{-\epsilon}$ is such that $s = 0$. \square

Now we are going to put together some results that we have mostly already proved in a proposition:

Proposition 2.31. Assume that y_K , as in (1.11), is not divisible by p in $E(K)/E(K)_{\text{tors}}$. Let l be a prime which is unramified in the extension M/\mathbb{Q} and such that there is a factor λ_M above it in M , whose Frobenius substitution equals τh in $\text{Gal}(M/\mathbb{Q})$, for some $h \in H$. Then $(l) = \lambda$ is inert in K and λ splits completely in $L = K(E_p)$.

The following are equivalent:

- a. $c(l) \equiv 0$ in $H^1(K, E_p)$,
- b. $c(l) \in \text{Sel}_p(E/K) \subset H^1(K, E_p)$,
- c. P_l is divisible by p in $E(K_l)$,
- d. $d(l) \equiv 0$ in $H^1(K, E)_p$,
- e. $d(l)_\lambda \equiv 0$ in $H^1(K_\lambda, E)_p$,
- f. $P_1 = y_K$ is locally divisible by p in $E(K_\lambda)$,
- g. $h^{1+\tau}$ lies in the subgroup $I^+ = H^+ \cap I$ of H^+ .

Proof. a. \Leftrightarrow b., since $c(l) \in H^1(K, E_p)^{-\epsilon}$, by (2.13) and $\text{Sel}_p(E/K)^{-\epsilon} = 0$ by lemma (2.30).

a. \Leftrightarrow c. by proposition (2.11). Always by proposition (2.11) since $(E(K)/pE(K))^{-\epsilon}$, by (2.30), we have $c(l) \equiv 0 \Leftrightarrow d(l) \equiv 0$ which means a. \Leftrightarrow d.

Since $d(l)$ is locally trivial except perhaps at λ and $\text{III}(E/K)_p^{-\epsilon} = 0$, by (2.30), we have d. \Leftrightarrow e. and e. \Leftrightarrow f., by (2.16).

Finally g. \Leftrightarrow e., since $\frac{1}{p} \in E(K_\lambda)$ is equivalent to the fact that λ splits completely in $L(\frac{1}{p}y_k)/K$, which is equivalent to the fact that the Frobenius substitution of the prime λ_M above λ in M/K is in I^+ , but $\text{Fr}_{\lambda_M/\lambda} = (\tau h)^2 = h^{1+\tau}$, so we are done. \square

Recall proposition (2.3).

Proposition. Let p be an odd prime such that the extension $\mathbb{Q}(E_p)/\mathbb{Q}$ has Galois group isomorphic to $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)$ modulo $E(K)_{\text{tors}}$. Then the group $\text{Sel}_p(E/K)$ is cyclic generated by $\delta(y_K)$.

The only thing we are missing is now:

Proposition 2.32. $\text{Sel}_p(E/K)^\epsilon \simeq \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$.

Proof. Let $s \in \text{Sel}_p(E/K)^\epsilon$. To show that s is a multiple of δy_K it suffices to show that $[s, \rho] = 0$ for all $\rho \in I$, for then $s \in \text{Hom}_{\mathcal{G}}(H/I, E_p) \simeq \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$. By the argument in proposition (2.28), which used the fact that E_p is simple as a \mathcal{G} -module, it is enough to show that $[s, \rho] = 0$ for all $\rho \in I^+$. These elements have the form $\rho = (\tau i)^2$, for $i \in I$, by proposition (2.27).

Let l' be a prime such that $c(l')$ is non trivial in $H^1(K, E_p)$; by proposition (2.31) condition g., we may obtain such an l' by imposing the condition that its Frobenius substitution is conjugate to $\tau h \in \text{Gal}(M/\mathbb{Q})$, where $h \in H$ and $h^{1+\tau} \notin I^+$. Then $c(l')$ is not in $\text{Sel}_p(E/K)$, by condition b. of the same proposition, so the extension $L' = L_{\langle c(l') \rangle}$, constructed as in (2.26), is disjoint from the extension M/L . A prime ideal $l\mathcal{O}_K = \lambda$ in K , which splits completely in L , is split completely in L' if and only if $K_{\lambda_{l'}} = K_\lambda$ for every prime $\lambda_{l'}$ lying above λ in L' . If we call $P_{l'} \in E(K)$ the element such that $\delta(P_{l'}) = c(l')$, then $L' = L(\frac{1}{p}P_{l'})$. So $\lambda \in K$ is split completely if and only if $\frac{1}{p}P_{l'} \in E(K_{\lambda_{l'}})$ is actually already in $E(K_\lambda)$, i.e. if and only if $P_{l'} \in pE(K_\lambda)$ which means $E(K_{\lambda_{l'}}) = K_\lambda$ for every $\lambda_{l'}$.

Now let l be a prime whose Frobenius substitution is conjugate to τi in $\text{Gal}(M/\mathbb{Q})$, with $i \in I$, and to τj in $\text{Gal}(L'/\mathbb{Q})$, where $j \in \text{Gal}(L'/L)$ satisfies $j^{1+\tau} \neq 1$. These conditions may be satisfied simultaneously, indeed we know that $M \cap L' = L$.

We claim that the class $d(ll') \in H^1(K, E)^\epsilon$ is locally trivial for all places $v \neq \lambda$, but that $d(ll')_\lambda \neq 0$.

Local triviality at primes $v \neq \lambda, \lambda'$, where $\lambda' = l'\mathcal{O}_K$, comes from proposition

(2.14). Since $i \in I$, the global class $c(l)$ is zero by (2.31), and so by condition c. P_l is divisible by p in $E(K_l)$. Hence it follows directly from proposition (2.16) that $d(l')_{\lambda'} = 0$. Finally $d(l')_{\lambda}$ is trivial if and only if P'_l is locally divisible by p in $E(K_{\lambda})$, but this implies that λ splits in L' , or equivalently that $(\tau j)^2 = j^{1+\tau} = 1$, which contradicts the hypothesis on j .

We may now apply proposition (2.24) to conclude that $s_{\lambda} = 0$, consequently

$$[s, \rho] = [s, (\tau i)^2] = 0.$$

Since, choosing l' ad hoc, this argument works for any $\rho \in I^+$ we have shown that $s(I^+) = s(I) = 0$. □

Acknowledgements

I would like to thank Prof. Jan Nekovár, for his advice, support and his rapid corrections during the redaction of this mémoire.

Bibliography

- [Art86] M. Artin. Néron models, arithmetic geometry (g. cornell, jh silverman, eds.), 1986.
- [CF67] J.W.S. Cassels and A. Frohlich. *Algebraic number theory*. Acad. Press, 1967.
- [Cox97] D.A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Wiley-Interscience, 1997.
- [DI95] F. Diamond and J. Im. Modular forms and modular curves. In *Seminar on Fermat's last theorem: 1993-1994, the Fields Institute for Research in the Mathematical Sciences, Toronto, Ontario, Canada*, volume 17, page 39. Amer Mathematical Society, 1995.
- [Gro] B.H. Gross. Kolyvagin work on modular elliptic curves. *L-functions and arithmetics*.
- [Gro84] B. Gross. Heegner points on $X_0(n)$. *Modular forms (Durham, 1983)*, Horwood, Chichester, pages 87–105, 1984.
- [GZ86] B. Gross and D. Zagier. Heegner points and derivatives of L -series. *Invent. math*, 84(2):225–320, 1986.
- [KM85] N.M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. Princeton Univ Pr, 1985.
- [Kna92] A.W. Knaapp. *Elliptic curves*, volume 40. Princeton Univ Pr, 1992.
- [Sil94] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer, 1994.
- [Sil09] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Verlag, 2009.
- [Was89] L. C. Washington. Number fields and elliptic curves. 265:245–278, 1989.